UNIVERZITA KARLOVA

Právnická fakulta

Anna Všetečková

Problematické aspekty ochrany osobních údajů

Diplomová práce

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

Katedra pracovního práva a práva sociálního zabezpečení

Datum vypracování práce (uzavření rukopisu) : 18. 12. 2017

Prohlašuji, že předloženou diplomovou práci jsem vypracovala samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu. Rovněž prohlašuji, že předkládaná diplomová práce má 198 280 znaků vlastního textu včetně poznámek pod čarou a mezer.

Anna Všetečková

V Praze dne

Děkuji tímto panu JUDr. Jakubu Morávkovi, Ph.D., vedoucímu mé diplomové práce, za ochotu vést mou diplomovou práci a za cenné připomínky a pomoc při jejím zpracování.

Obsah

ÚVOD

Zajištění ochrany osobních údajů je jedním ze zásadních problémů, se kterým se musí lidská civilizace ve 21. století vypořádat. Ačkoli je význam ochrany osobních údajů širokou veřejností často podceňován až bagatelizován, může být v důsledku jejich zneužití zcela zásadně zasaženo do života jednotlivce a jeho soukromí. Právo na nedotknutelnost osoby a soukromí je přitom jako základní lidské právo zakotveno nejen v právním řádu České republiky a právu Evropské unie, ale i v právních řádech ostatních vyspělých demokratických právních států. V rámci tuzemského právního řádu je pak právo na soukromí a právo na ochranu před zneužíváním osobních údajů garantováno na nejvyšší úrovni v rámci ústavního pořádku. Stejně tak je v rámci práva Evropské unie právo na ochranu osobních údajů uvedeno v Listině základních práv Evropské unie, která je primárním pramenem práva. Nejen ze systematického zařazení práva na ochranu osobních údajů lze dovodit, že jak český, tak i evropský zákonodárce si význam ochrany osobních údajů a důležitost důsledné úpravy nakládání s nimi plně uvědomují.

Lze bezpochyby konstatovat, že význam ochrany osobních údajů značně vzrostl v důsledku masového rozšíření výpočetních technologií. Stolní počítače se staly běžnou součástí domácností i podniků a ukládání, třídění a další zpracovávání osobních údajů se podstatně zjednodušilo. Automatizované zpracování osobních údajů za pomoci software otevřelo dveře pro moderní pojetí marketingu a obchodních strategií, které umožňovaly na základě získaných údajů lépe něž kdy předtím vymezit cílovou skupinu a realizovat efektivní prodej.

V českých podmínkách pak lze za další mezník pro význam regulace ochrany osobních údajů považovat přechod na systém tržního hospodářství, kdy velká skupina subjektů začala zpracovávat osobní údaje v rámci podnikání.

Za poslední skutečnost pro ochranu osobních údajů zcela zásadního charakteru lze označit rozšíření užívání internetu pro soukromé účely. Uživatelé internetu jeho prostřednictvím nakupují, vyhledávají informace pro profesní i čistě soukromé účely,

komunikují mezi sebou a nebojí se projevit své nejniternější potřeby a názory. Anonymita a nevystopovatelnost uživatelů internetu je přitom pouze zdánlivou kategorií, kdy za pomocí legálních (technologie tzv. cookies) i protiprávních (hacking) metod lze aktivity uživatele vystopovat a zasáhnout tak do jeho intimní sféry. Zvláštní a zvlášť významnou kapitolou jsou sociální sítě a aktivita jejich uživatelů, kteří na nich dobrovolně uveřejňují značné množství osobních údajů. Ty pak mohou být zneužity jak ze strany provozovatelů těchto sociálních sítí, tak i ostatními uživateli.

Vzhledem k významu komunikačních technologií z hlediska ochrany osobních údajů a jejich rychlému vývoji je bezpodmínečně nutné sledovat jejich současný stav a při tvorbě právních norem pružně reagovat na aktuální dění. Český i evropský zákonodárce tak čelí poměrně nevděčnému úkolu, kdy musí zajistit vysokou úroveň ochrany osobních údajů nejen pro stav současný, ale i budoucí. Právo ochrany osobních údajů je proto velmi dynamicky se vyvíjejícím právním odvětvím.

Ačkoli si to řada jednotlivců neuvědomuje, jsou osobní údaje velice citlivou a pro určité skupiny osob i cennou a žádanou komoditou. Mnoho podnikatelů je připraveno investovat do reklamy a marketingu nemalé finanční částky a informace o jejich potencionálních zákaznících potřebné pro správné cílování jejich nabídky jsou proto velice žádaným zbožím. Motivace pro zasažení do intimní sféry osob a zneužití jejich osobních údajů je proto bezesporu přítomna. Vedle zneužití osobních údajů jednotlivci čistě pro individuální účely je možné uvažovat i o systematickém zneužívání osobních údajů prováděných státy, resp. určitými mocenskými elitami, a to za účelem identifikace či likvidace případných opozičních sil.

Tradičním případem, kdy dochází ke zpracování značného množství osobních údajů, je výkon závislé práce. Závislá práce je vykonávána v pracovněprávním vztahu, kdy je zaměstnavatel povinen pro řádné plnění zákonem mu uložených povinností zpracovávat osobní údaje svých zaměstnanců. Zaměstnavatel tak zpracovává osobní údaje nejen v situacích, ze kterých těží převážně zaměstnanec[1], ale rovněž pro čistě

[1] Např. zpracování osobních údajů za účelem výplaty mzdy či platu.

vlastní potřebu.[2] Povaha zpracovávaných údajů přitom může být značně intimní, jako tomu například je při zpracování údajů o zdravotním stavu zaměstnance. Vzhledem ke skutečnosti, že většina populace je odkázána na příjmy ze závislé činnosti, má ochrana osobních údajů v pracovněprávních vztazích zcela zásadní charakter.

Lze tedy shrnout, že ochrana osobních údajů není pouze jakousi nadstavbovou a v běžném životě nepřítomnou disciplínou, ale naopak velmi aktuálním a konkrétním problémem, který je nutné efektivně řešit. Stanovení jasných a přiměřených pravidel pro nakládání s osobními údaji a zajištění jejich ochrany je tak nanejvýš potřebné. Autorka práce rozhodně nemá v úmyslu samotný institut zpracování osobních údajů démonizovat, naopak je přesvědčena o jeho výhodnosti jak pro subjekt údajů, tak pro správce, považuje ovšem za nezbytné vymezení jasných pravidel a jejich důsledné dodržování.

Cílem této diplomové práce není poskytnout vyčerpávající přehled problematiky osobních údajů a jejich ochrany, ale podrobněji rozebrat vybrané instituty práva ochrany osobních údajů jak z hlediska v současné době platné a účinné právní úpravy, tak optikou Obecného nařízení na ochranu osobních údajů, jež vstupuje v účinnost dne 25. května roku 2018. Autorka se bude věnovat nejen komparaci současného stavu s úpravou obsaženou v Obecném nařízení na ochranu osobních údajů, ale rovněž analýze některých nových institutů, které Obecné nařízení přináší, spolu s nastíněním možných problematických aspektů a jejich řešení. Autorka se stejně tak pokusí o celkové vyhodnocení „nové“ právní úpravy a jejích důsledků pro právo ochrany osobních údajů.

[2] Např. sledování zaměstnanců za účelem ochrany majetku zaměstnavatele.

I. PRAMENY PRÁVNÍ ÚPRAVY

Prameny práva lze obecně dělit na prameny ve smyslu formálním a materiálním. Za materiální prameny práva lze obecně označit určité mimoprávní skutečnosti, které stát vedou k úpravě vztahů pomocí právních norem. Formálním pramenem práva se pak rozumí státem upravená, resp. uznaná forma, v jaké může být obsah právní normy zachycen. V této kapitole se budu věnovat pramenům práva ve formálním smyslu.

V této kapitole jsem se rozhodla zvolit částečně netradiční řazení jednotlivých pramenů práva, které v literatuře zpravidla postupuje podle právní síly a prvně shrnuje mezinárodní právní akty, následně se věnuje pramenům práva v rámci Evropské unie a teprve jako poslednímu se věnuje právnímu řádu České republiky. Právo na ochranu osobních údajů je však oblastí, v níž se Evropská unie rozhodla přistoupit k unifikaci právních předpisů jednotlivých členských států, a to konkrétně přijetím Obecného nařízení. Vzhledem ke skutečnosti, že nařízení je přímo použitelné a není nezbytné jej do právního řádu jednotlivých členských států transponovat prostřednictvím jiného právního předpisu, jako je tomu např. u směrnic, z hlediska právní síly jej lze při zohlednění jeho zvláštní povahy postavit na úroveň zákonů České republiky.

První podkapitola se věnuje základům mezinárodní, evropské a české právní úpravy, které tvoří mezinárodní právní akty, primární prameny práva Evropské unie a ústavní pořádek České republiky. Z nich následně vychází sekundární prameny práva Evropské unie a zákonné právní předpisy České republiky, jimž se věnuje podkapitola druhá. V ní je pozornost věnována nejen současné právní úpravě, tedy zákonu č. 101/2000 Sb., o ochraně osobních údajů a Směrnici 95/46/ES, kterou tento zákon provádí, ale i právní úpravě nové, a to Obecnému nařízení a návrhu zákona o zpracování osobních údajů.

1.1 ZÁKLADY MEZINÁRODNÍ, EVROPSKÉ A ČESKÉ PRÁVNÍ ÚPRAVY

1.1.1 MEZINÁRODNÍ PRÁVO

Jak vyplývá z čl. 10 Ústavy, vyhlášené mezinárodní smlouvy, k jejichž ratifikaci dal Parlament souhlas a jimiž je Česká republika vázána, tvoří součást právního řádu

České republiky, přičemž mají aplikační přednost vůči zákonu, zákon s nimi tedy musí být v souladu.

Stejně jako je tomu v českém právním řádu, tak i mezinárodní právo upravuje obecnou nedotknutelnost osoby a jejího soukromí. Je tomu tak zejména ve Všeobecné deklaraci lidských práv, v Mezinárodním paktu o občanských a politických právech a Evropské úmluvě o ochraně lidských práv a základních svobod.

Všeobecná deklarace lidských práv byla přijata na půdě Organizace spojených národů Valným shromážděním v roce 1948. Je však nutné poznamenat, že nemá povahu mezinárodní smlouvy a na její znění se tak nelze přímo odvolávat v rámci horizontálních právních vztahů.[3]

Ačkoliv je právo na ochranu před zásahy nebo útoky do soukromého života člověka zakotveno zejména v čl. 12 Všeobecné deklarace lidských práv[4], východisko pro ochranu soukromí člověka nalezneme již v čl. 3, jenž stanoví že každý má právo na život, svobodu a osobní bezpečnost. Tento článek je nezbytné vykládat tak, že každý má právo žít život dle vlastních představ, a to bez zásahů do svého soukromí.[5] Pro oblast pracovněprávních vztahů je pak nutné zmínit i čl. 17, který každému, tedy i zaměstnavateli, zaručuje právo vlastnit a chránit svůj majetek a čl. 23 odst. 1, který každému přiznává právo na práci, svobodnou volbu zaměstnání, na spravedlivé a uspokojivé pracovní podmínky a na ochranu proti nezaměstnanosti.

V roce 1966 pak byly přijaty Mezinárodní pakt o občanských a politických právech a Mezinárodní pakt o hospodářských, sociálních a kulturních právech, které již mají

---

[3] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 86.

[4] *„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“.*

[5] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 84.

formu mezinárodních smluv. Jejich přijetím vyvrcholily snahy Organizace spojených národů o přijetí hodnot vyjádřených ve Všeobecné deklaraci lidských práv formou *hard-law*.[6] Právo na ochranu lidské důstojnosti a soukromí člověka nalezneme zakotveno v čl. 17 Mezinárodního paktu o občanských a politických právech, právo na uspokojivé pracovní podmínky je pak výslovně vyjádřeno v čl. 7 Mezinárodního paktu o hospodářských, kulturních a sociálních právech.

Vedle Organizace spojených národů dále není možné opomenout ani činnost Rady Evropy. V oblasti základních lidských práv pak hraje nepopiratelnou rolu touto organizací přijatá Úmluva o ochraně lidských práv a základních svobod z roku 1950[7], která v čl. 8 zakotvuje právo každého člověka na respektování soukromí a na ochranu před zásahy do něj. Právo na ochranu vlastnictví se pak zaručuje v čl. 1 Dodatkového protokolu č. 1 k Úmluvě o ochraně lidských práv a základních svobod.

Vedle Úmluvy o ochraně lidských práv a základních svobod nelze pominout ani význam usnesení Rady Evropy Resolution (73) 22[8] a Resolution (74) 29[9], která se věnovala zejména principům ochrany soukromí osob při vytváření elektronických databank, a jejichž nepřímým cílem bylo iniciovat vznik národních úprav pro vytváření elektronických datových souborů.[10] Ačkoliv se některé státy této

---

[6] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 87.

[7] Úmluva o ochraně lidských práv a základních svobod byla prvními signatáři podepsána v Římě v roce 1950, přičemž v platnost vstoupila v roce 1953.

[8] Resolution (73) 22 on the protection of privacy of individual vis-à-vis electionic data banks in the private sector.

[9] Resolution (74) 29 on the protection of individual vis-à-vis electionic data banks in the public sector.

[10] ŠMÍD, V. *Ochrana osobních údajů v pracovněprávních vztazích*. 2003, dostupné na http://www.fi.muni.cz/~smid/oouppv.html .

iniciativy chopily a vnitrostátní úpravu na ochranu dat přijaly, bylo zřejmé, že v této oblasti bude nezbytná spolupráce mezi státy a přijetí mezinárodních standardů.[11]

V souvislosti s tím nelze pominout činnost Organizace pro hospodářskou spolupráci a rozvoj (OECD), která jako první upravila základní pojmy a principy ochrany osobních údajů, a to v dokumentu Doporučení pro ochranu soukromí a toky osobních údajů přes hranice z roku 1980. Tento dokument však má povahu *soft-law*, je tak spíše doporučující povahy a nemá povahu závazného pramene práva.

V oblasti ochrany osobních údajů však hraje zásadní roli Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108 z roku 1981.

Úmluvu č. 108 ratifikovala Česká republika až v roce 2000, kdy byl přijat zákon č. 101/2000 Sb., o ochraně osobních údajů, který byl na rozdíl od předchozího zákona o ochraně osobních údajů v informačních systémech již plně konformní s Úmluvou č. 108. Jak už celý název Úmluvy č. 108 napovídá[12], aplikovala se původně na automatizované soubory dat a automatizované zpracování osobních dat ve veřejném i soukromém sektoru. V roce 2003 však vstoupilo v platnost prohlášení České republiky[13], které rozšířilo působnost Úmluvy i na soubory osobních údajů, které se nezpracovávají automatizovaně.

Zásadním přínosem Úmluvy č. 108 byla skutečnost, že jako první v oblasti *hard-law* definovala zásadní pojmy jako osobní údaj, subjekt osobních údajů, automatizovaný soubor dat, automatizované zpracování a správce osobních údajů. Rovněž zavedla

---

[11] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 96.

[12] Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108 z roku 1981.

[13] JANEČKOVÁ, E., BARTÍK, V. *Ochrana osobních údajů v pracovním právu (Otázky a odpovědi)*. Praha: Wolters Kluwer, 2016, s. 12.

základní principy ochrany osobních údajů, z nichž následně vycházela i Směrnice 95/46/ES.[14]

1.1.2 PRIMÁRNÍ PRÁVO EVROPSKÉ UNIE

Zásadní roli pro určování podoby práva na ochranu osobních údajů hraje právo Evropské unie, jenž usiluje o harmonizaci v této oblasti ve všech členských státech. Činí tak prostřednictvím primárních i sekundárních pramenů práva, zejména prostřednictvím nařízení a směrnic.

Pravomoc vytvářet a přijímat právně závazné akty v oblasti práva na ochranu osobních údajů si Evropská unie vyhrazuje v čl. 16 Smlouvy o fungování Evropské unie[15]. Listina základních práv Evropské unie dále řadí právo na ochranu osobních údajů mezi základní práva a svobody Evropskou unií uznávané, a to konkrétně v čl. 8[16]. Oba

---

[14] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 105.

[15] „*Článek 16*

(bývalý článek 286 Smlouvy o ES)

1. *Každý má právo na ochranu osobních údajů, které se jej týkají.*
2. *Evropský parlament a Rada přijmou řádným legislativním postupem pravidla o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů. Dodržování těchto pravidel podléhá kontrole nezávislými orgány.*
3. *Pravidly přijatými na základě tohoto článku nejsou dotčena zvláštní pravidla uvedená v článku 39 Smlouvy o Evropské unii.“*

[16] „*Článek 8*

Ochrana osobních údajů

1. *Každý má právo na ochranu osobních údajů, které se ho týkají.*
2. *Tyto 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.*
3. *Na dodržování těchto pravidel dohlíží nezávislý orgán.“*

zmíněné předpisy upravují právo na ochranu osobních údajů konkrétně a nikoliv pouze obecně jako součást práva na ochranu soukromí.

1.1.3 ÚSTAVNÍ POŘÁDEK

Základním východiskem pro český právní řád je ústavní pořádek, jehož součást tvoří i Listina základních práv a svobod.

LZPS se ochrany osobních údajů dotýká hned ve dvou svých článcích, a to v čl. 7 a v čl. 10. Čl. 7 odst. 1 LZPS je ustanovením, které zaručuje všem osobám bez ohledu na jejich občanství právo na nedotknutelnost osoby a jejího soukromí. Čl. 10 LZPS pak čl. 7 konkretizuje a zabývá se již přímo ochranou osobnosti člověka.

Ústavní soud již v minulosti dovodil, že právo jednotlivce rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům je jedním ze základních aspektů práva na soukromí, a to v podobě práva na informační sebeurčení.[17] Tzv. právo na informační sebeurčení je pak výslovně zakotveno v čl. 10 odst. 3 LZPS, který stanoví, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

Z dikce ustanovení čl. 10 odst. 3 LZPS vyplývá, že soukromí není chráněno proti zásahům, k nimž existuje zákonná licence.

Pojem soukromí však není v žádném právním předpisu definován. Z jeho povahy vyplývá, že se nejedná o jednotné právo, nýbrž o komplex práv, která chrání osobu člověka. Patří mezi ně zmíněné právo na ochranu osobních údajů, ale i právo na ochranu rodiny, nedotknutelnosti osobnosti, ochrana obydlí, právo na zachování nedotknutelnosti intimní sféry, sexuálního života a sexuální orientace, apod.[18]

---

[17] Nález Ústavního soudu České republiky ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10.

[18] MATES, Pavel. *Ochrana soukromí ve správním právu*. 2., aktualiz. a podstatně přeprac. vyd. Praha: Linde, 2006, s. 20.

Právo na ochranu soukromí však často přichází do konfliktu s dalšími ústavně zaručenými právy, a to zejména s vlastnickým právem a s právem na informace.

Pod pojmem právo na informace LZPS rozumí právo informace vyhledávat a šířit. Čl. 16, jenž právo na informace upravuje, dále doplňuje zákon č. 106/1999 Sb., o svobodném přístupu k informacím, jenž upravuje pravidla pro poskytování informací státními orgány a orgány územní samosprávy a dále podmínky práva svobodného přístupu k těmto informacím. LZPS sama předpokládá, že právo na informace není právem bezbřehým a lze jej ve vymezených případech omezit zákonem.[19] K takovému omezení dochází i z důvodu ochrany jiných osob a jejich osobních údajů.

Pojem informace nelze ztotožňovat s pojmem osobní údaj. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, pojem informace definuje jako jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního. Lze tedy říci, že informace se stává osobním údajem pouze v případě, kdy je předmětem této informace fyzická osoba.[20]

Dalším základním právem, jenž často přichází do konfliktu s právem na ochranu soukromí, je vlastnické právo. Z důvodu jeho ochrany se vlastník často uchyluje k umístění kamerových systémů a následnému sledování osob, tedy ke zpracování jejich osobních údajů. I zde je však nutné zjišťovat, zda je v daném případě takovýto zásah do soukromí osoby vhodný, potřebný a přiměřený.

---

[19] Čl. 16 odst. 4 LZPS.

[20] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. Beckova edice ABC, s. 5.

1.2 DALŠÍ PRÁVNÍ PŘEDPISY

1.2.1 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, upravuje základní principy a povinnosti vznikající při zpracování osobních údajů a jejím úkolem je zajistit jejich dodržování ve všech legislativách jednotlivých členských států. Důležitým důvodem pro vznik unijní úpravy ochrany osobních údajů byl stále častější pohyb údajů mezi jednotlivými členskými státy. Aby mohlo dojít k vytvoření fungujícího vnitřního trhu, v němž mohou jednotlivé podniky efektivně spolupracovat, bylo nutné přijmout stejnou míru ochrany občanů ve všech členských státech.

Základní principy, na nichž Směrnice stojí, jsou vymezeny již v úvodních recitálech, jichž je celkem 72. Samotnou Směrnici pak tvoří dalších 34 článků.

Směrnice se vztahuje na systematické zpracování osobních údajů, a to jak automatizované, tak prováděné jinými prostředky, přičemž je nutné, aby na základě zpracovávaných údajů bylo možné za užití rozumného množství prostředků fyzické osoby identifikovat.[21]

Jak již bylo výše uvedeno, Směrnice 95/46/ES byla transponována do českého právního řádu prostřednictvím OchOsÚ a základní povinnosti, které obsahuje, již známe z OchOsÚ. Ve svých obecných ustanoveních obdobně jako Úmluva 108 definuje základní pojmy, se kterými pak dále pracuje, jako jsou osobní údaj, zpracování osobních údajů a správce a zpracovatel. Mezi základní povinnosti správce, které Směrnice zavádí, patří povinnost zpracovávat osobní údaje pouze na základě řádného právního titulu, stanovit účel zpracování osobních údajů, řádně zabezpečit osobní údaje, dodržet informační povinnost vůči subjektu údajů a rovněž plnit povinnosti ohledně předávání osobních údajů do třetích zemí.

[21] Recitál 26 Směrnice 95/46/ES.

Důležitou povinností je i oznamovací povinnost správců vůči orgánu dozoru a s tím související povinnost členských států takový orgán vytvořit a pověřit jej vedením veřejného seznamu registrovaných osob. Ačkoliv Směrnice 95/46/ES ve svém čl. 18 stanoví, že se oznamovací povinnost vztahuje pouze na automatizované zpracování osobních údajů, Česká republika využila možnosti, kterou dává odst. 6 stejného ustanovení, a oznamovací povinnost vztahuje i na neautomatizované zpracování osobních údajů. V České republice funkci orgánu dozoru plní Úřad pro ochranu osobních údajů, jenž je nezávislým ústředním správním úřadem.[22]

Zásadní roli hraje čl. 29 a násl. Směrnice, na jehož základě byla zřízena pracovní skupina WP29 (zkratka z anglického *„working party"* a čísla čl. 29)[23]. WP29 je nezávislým orgánem a jejím úkolem je plnění poradní funkce. Ta je blíže vymezena čl. 30 a spočívá zejména v (a) posuzování veškerých otázek týkajících se uplatňování vnitrostátních právních předpisů; (b) zaujímání stanoviska o úrovni ochrany v EU a členských zemích; (c) poskytování poradenství o všech návrzích změn Směrnice; a zaujímání stanoviska ke kodexům chování vypracovaných na úrovni EU. Rovněž má WP29 povinnost uvědomit Komisi EU o rozporu mezi právními předpisy a praxí členských států, které by mohly narušit rovnocennost ochrany osob v souvislosti se zpracováním osobních údajů.

Směrnice byla přijata v roce 1995, tedy ještě před masivním rozvojem výpočetní techniky a užíváním internetu širokou veřejností. Z tohoto důvodu začalo být zřejmé, že je nutné přikročit k nastavení nového právního rámce ochrany osobních údajů.[24] Po rozsáhlých diskuzích bylo přikročeno k řešení současného stavu přijetím zcela

---

[22] § 2 odst. 3 OchOsÚ, přičemž povinnost členských států zřídit orgán dozoru je zakotvena v ustanovení čl. 28 odst. 1 Směrnice 95/46/ES.

[23] Oficiální internetové stránky WP 29 jsou dostupné na následujícím odkazu: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[24] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 153.

nové právní úpravy, a to prostřednictvím Obecného nařízení. Nařízení nabývá účinnosti dne 25. května 2018 a k tomuto dni se rovněž ruší Směrnice 95/46/ES.

1.2.2 OBECNÉ NAŘÍZENÍ

Jak již bylo zmíněno, hlavním důvodem pro přijetí nového nařízení byla skutečnost, že Směrnice 95/46/ES byla přijata před rychlým technologický rozvojem a s ním souvisejícím vzrůstajícím objemem sdílených osobních údajů. Je tedy důležité zajistit jejich vysokou ochranu při jejich předávání mezi jednotlivými členskými státy, a to na úrovni celé Evropské unie, jelikož se jedná o základní právo Evropskou unií zajištěné. Z důvodu zajištění unifikace právních řádů jednotlivých členských států a zvýšení právní jistoty občanů byla zvolena forma nařízení, které je přímo použitelné.

Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES, se vztahuje na všechny způsoby zpracování osobních údajů, tedy jak na automatizované, tak manuální zpracování údajů, které mají být uloženy v evidenci. Zároveň však Obecné nařízení pamatuje na skutečnost, že existují oblasti, na které se právo Evropské unie nevztahuje a nemělo by je tedy upravovat ani nařízení, jako je například zpracovávání osobních údajů prováděné v oblasti bezpečnosti státu.[25]

V platnosti zůstává princip, že se chrání pouze osobní údaje fyzických osob, a to takové, na jejichž základě je osobu možné identifikovat, nikoliv tedy údaje, které byly dostatečně anonymizovány tak, aby subjekt údajů již nebyl identifikovatelný.[26]

Vedle výše zmíněných však Nařízení přináší i některé další, v této oblasti zcela nové instituty. Mezi ně patří zejména zavedení institutu tzv. pověřence pro ochranu

---

[25] Srov. Důvodová zpráva k Návrhu nařízení Evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) ze dne 25. 1. 2012, COM/2012/010 final - 2012/0010 (COD).

[26] Recitál 26 Obecného nařízení.

osobních údajů. Neméně důležité jsou značné změny pro činnost správce při zpracovávání osobních údajů nebo před tímto zpracováváním. Správce bude nově zatížen celou další řadou povinností, jako je posouzení vlivu na ochranu osobních údajů nebo nutnost konzultace zpracování s dozorovým úřadem.

Obecné nařízení obdobně jako Směrnice 95/46/ES stanoví, že každý členský stát je povinen pověřit jeden nebo více nezávislých orgánů veřejné moci výkonem funkce dozorového úřadu v oblasti ochrany osobních údajů.[27] Je téměř jisté, že v České republice bude dozorovým úřadem opět ÚOOÚ, což předpokládá i návrh zákona o zpracování osobních údajů.[28]

Obecné nařízení v čl. 68 zřizuje nový subjekt, a to Evropský sbor pro ochranu osobních údajů, který by měl nahradit současnou WP29.[29] Hlavním úkolem Evropského sboru je zajištění jednotného uplatňování Obecného nařízení, a to např. poskytováním poradenství Evropské komisi nebo vydáváním pokynů, doporučení a osvědčených postupů.[30]

Nařízení nutně přinese některé změny i do českých právních předpisů, zejména do OchOsÚ, který bude zřejmě nahrazen zcela novým zákonem o zpracování osobních údajů. Vzhledem ke skutečnosti, že nařízení má přímý účinek, není již nutné práva a povinnosti v něm stanovená upravovat rovněž na národní úrovni. Obecné nařízení u některých institutů samo předpokládá, že budou upraveny na vnitrostátní úrovni, jako je zpracování osobních údajů pro účely výkonu svobody projevu, práva na informace, svobody vědeckého bádání a umělecké tvorby, nebo zpracování osobních údajů v souvislosti se zaměstnáním. Tyto instituty však zřejmě budou upraveny zvláštními zákony, jako je například ZPr, a nikoliv přímo zákonem o zpracování osobních údajů.

---

[27] Čl. 51 odst. 1 Obecného nařízení.

[28] § 45 návrhu zákona o zpracování osobních údajů.

[29] Recitál 139 Obecného nařízení.

[30] Čl. 68 odst. 1 Obecného nařízení.

Současně s Obecným nařízením byly přijaty další dvě směrnice důležité pro oblast osobních údajů, a to Směrnice Evropského parlamentu a Rady 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, a Směrnice Evropského parlamentu a Rady 016/681 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.

1.2.3 ZÁKONY

Prvním právním předpisem, který kdy na našem území ochranu osobních údajů upravoval, byl v Československu přijatý zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Zásadní inspirací pro výše zmíněný zákon byla Úmluva č. 108. Zákon však v praxi nebyl příliš respektován, a to zejména z důvodů, že nestanovil žádné efektivní sankce za jeho porušování a zároveň nezřizoval žádný nezávislý orgán, který by na jeho dodržování dohlížel.[31]

Tyto vady byly napraveny až v roce 2000, kdy byl přijat v současnosti účinný OchOsÚ. Tento zákon byl přijat v souvislosti se vstupem České republiky do Evropské unie, v jehož důsledku vznikla nutnost přizpůsobení českých právních předpisů právě předpisům Evropské unie, a to zejména Směrnici 95/46/ES.

OchOsÚ je obecným právním předpisem, který vymezuje jednotlivé pojmy relevantní pro ochranu osobních údajů, upravuje základní principy, jimiž se ochrana osobních údajů řídí a zakotvuje postavení ÚOOÚ.

[31] MATES, Pavel. *Ochrana soukromí ve správním právu*. 2., aktualiz. a podstatně přeprac. vyd. Praha: Linde, 2006, s. 188.

Samotné zpracování osobních údajů je pak upraveno v celé řadě dalších právních předpisů. Je nutné zmínit zejména zákon č. 262/2006 Sb., zákoník práce, jenž upravuje možnosti zaměstnavatele k zasahování do soukromí zaměstnance či zákon č. 480/2004 Sb., o některých službách informační společnosti, jenž upravuje zasílání obchodních sdělení.

OchOsÚ byl za dobu své účinnosti již několikrát novelizován a v souvislosti s přijetím Obecného nařízení bude nahrazen zcela novým právním předpisem. Návrh znění nového zákona s názvem „zákon o zpracování osobních údajů“ dokončilo v létě roku 2017 Ministerstvo vnitra České republiky a k okamžiku vypracování této práce zatím neprošel řádným legislativním procesem. Lze tedy předpokládat, že současné znění tohoto návrhu projde ještě četnými změnami.

Je ovšem namístě položit si otázku, jakým způsobem by byla řešena situace, pokud by se výše uvedený návrh zákona reflektující a konkretizující právní úpravu obsaženou v Obecném nařízení nepodařilo do nabytí účinnosti Obecného nařízení přijmout. Vzhledem ke skutečnosti, že nová evropská úprava ochrany osobních údajů má formu nařízení, které je dle evropského práva v členských státech přímo a bezprostředně účinné, není nutné Obecné nařízení implementovat do právních řádů jednotlivých členských států a evropská právní úprava se použije bez ohledu na jejich legislativní činnost.

Výše uvedené ovšem nijak nevyučuje možnost rozporu mezi dosavadními tuzemskými právními předpisy a novou evropskou úpravou. Takovou situaci by bylo nutné vyřešit za použití základních zásad evropského práva, konkrétně zásady aplikační přednosti. Předmětná zásada dopadá na situace, kdy nastane kolize při aplikaci evropského práva a práva národního. Pokud se dle ní dostane přímo použitelná norma práva evropské unie do aplikační kolize s normou práva členského státu, má norma evropského práva aplikační přednost. Na základě výše uvedeného pak lze shrnout, že v případě, kdy by se zákon o zpracování osobních údajů nepodařilo přijmout před účinností Obecného nařízení, lze nastalou situaci vyřešit použitím

zásady aplikační přednosti, kdy se normy odporující předpisům Evropské unie v daném rozsahu nepoužijí.

Právní předpisy, které nejsou s evropskou právní úpravou v souladu, ovšem nadále zůstávají součástí právního řádu, a mohou tak být příčinou právní nejistoty povinných subjektů. Zákonodárce by proto měl dbát na to, aby právní řád byl v souladu s aktuální evropskou legislativou.

Dalším způsobem, jakým lze odstranit nesoulad mezi normou vnitrostátního původu a normou evropského práva je použití tzv. eurokonformního výkladu. Členské státy mají povinnost zajistit, aby orgány veřejné moci (včetně soudů) vykládaly vnitrostátní právní normy tím, způsobem, aby bylo dosaženo požadavků stanovených evropským právem.[32] Povinnost použití eurokonformního výkladu pak přichází v úvahu především v těch případech, kdy nelze uvažovat o přímém účinku evropského práva.[33] V duchu výše uvedené zásady je proto nutno při interpretaci vnitrostátních předpisů na tyto předpisy pohlížet rovněž optikou evropského práva, což samozřejmě platí i v oblasti práva ochrany osobních údajů. Pokud by nedošlo k včasnému přijetí zákona o zpracování osobních údajů, mohly by tak použitím eurokonformního výkladu být odstraněny nesrovnalosti mezi evropskou a vnitrostátní právní úpravou, zastoupenou zejména OchOsÚ. Na druhou stranu povinnost eurokonformního výkladu za současné absence odpovídající vnitrostátní úpravy s sebou nese značné riziko vzniku právní nejistoty, a včasné přijetí národního předpisu, který zohlední evropskou úpravu, se jeví jako nanejvýš vhodné.

[32] Rozsudek SDEU ve věci C – 212/04, Konstantinos Adeneler a další v. Ellinikos Organismos Galaktos (ELOG), bod 117.

[33] Rozsudek SDEU ve věci C – 212/04, Konstantinos Adeneler a další v. Ellinikos Organismos Galaktos (ELOG), bod 113.

II. ZÁKLADY PRÁVNÍ ÚPRAVY OCHRANY OSOBNÍCH ÚDAJŮ

2.1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

Z původního vymezení základních pojmů stěžejních pro ochranu osobních údajů, které provedla již Směrnice o ochraně soukromí a přeshraničních tocích osobních údajů a následně i Úmluva 108, vychází i aktuální právní předpisy. Směrnice 95/46/ES, OchOsÚ a rovněž Obecné nařízení se od zavedených definic odchylují pouze minimálně.

2.1.1 OSOBNÍ ÚDAJ

Základním pojmem, který provází celé právo na ochranu osobních údajů, je pojem osobní údaj. V OchOsÚ je definován následovně: „*Osobním údajem (se rozumí) jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*.“ Obdobnou definici obsahují i Směrnice 95/46/ES a Obecné nařízení, přičemž Obecné nařízení demonstrativní výčet jednotlivých osobních údajů doplňuje o lokační údaje, síťový identifikátor, či jiný zvláštní prvek specifický pro genetickou identitu subjektu údajů.

Osobní údaj je širokým pojmem, jenž má zahrnout veškeré informace, které mohou s fyzickou osobou souviset, a to jak o informace objektivní, tak o informace subjektivní, jako jsou názory a hodnocení.[34]

Jak z výše uvedené definice vyplývá, za osobní údaje se považují takové informace, na jejichž základě může být osoba identifikována, a to jak přímo, tak nepřímo. Rozdíl mezi přímou a nepřímou identifikací spočívá v tom, že přímou identifikací je možné zjistit identitu osoby jednoznačně na základě přesného identifikátoru. Za takové údaje

[34] WP29 Opinion 4/2007 on the Concept of Personal Data (*překlad vlastní*).

se považují zejména jméno, příjmení, adresa a datum narození, případně jejich kombinace. Na rozdíl od toho se za nepřímou identifikaci považuje identifikace na základě jakékoliv jiné kombinace údajů, která umožňuje od sebe jednotlivé osoby odlišit.[35]

Pojem určitelnost, jenž je pro definici osobního údaje stěžejní, lze chápat jako stav, kdy lze na základě dostupných informací fyzickou osobu jasně odlišit od jiných fyzických osob. Posouzení toho, zda jsou tyto identifikátory dostačující pro určení osoby, se bude vždy odvíjet od konkrétní situace. Například jméno a příjmení, které jsou v praxi nejčastěji používány jako metody identifikace osoby, nemusí být v případě běžně rozšířených jmen pro určení konkrétní osoby dostačující.

Při posuzování, zda se subjekt na základě dostupných údajů považuje za určitelný, je nutné přihlédnout ke všem prostředkům, které by pro provedení identifikace musely být použity[36], přičemž lze předpokládat, že správce ani zpracovatel nebudou vyvíjet nadměrné úsilí a nevynaloží nadměrné náklady k identifikaci osoby.

Novou kategorii osobních údajů, jež zavádí Obecné nařízení, jsou údaje pseudonymizované. Pseudonymizace je v čl. 4 bodu 5) Obecného nařízení definována jako *„zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě“*. Určení, jaké osoby se pseudonymizované údaje týkají, tedy není možné provést přímo a je nutné použití dodatečných informací. Není vyloučeno, aby doplňkové informace, které umožní identifikaci osoby, uchovával sám správce, avšak

[35] Stanovisko ÚOOÚ č. 3/2012 k pojmu osobní údaj.

[36] Užití kritéria, kdy je při posuzování určitelnosti nutné přihlédnout ke všem prostředkům, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby, předpokládá ve svých recitálech jak Směrnice 95/46/ES, a to v recitálu č. 26, tak Obecné nařízení, rovněž v recitálu č. 26.

pokud tak činí, je povinen zajistit, aby byly uchovávány odděleně od samotných pseudonymizovaných údajů.

Výslovné zavedení pojmu pseudonymizace do Obecného nařízení má dle recitálů č. 26 a 28 za cíl zvýšit ochranu subjektů osobních údajů a rovněž napomoci správcům a zpracovatelům při plnění jejich povinností, a to zejména povinností v oblasti zabezpečování údajů.

Pseudonymizované údaje je nutné odlišovat od údajů anonymizovaných. Anonymizované údaje jsou údaje upravené tak, že subjekt údajů na jejich základě není nebo již přestal být identifikovatelným. Z důvodu, že anonymizované údaje není možné přiřadit ke konkrétnímu subjektu údajů, není nutné tomuto subjektu ani poskytovat ochranu osobních údajů. Obecné nařízení ani jiné právní předpisy se tak na anonymizované údaje nevztahuje.

2.1.2 ZVLÁŠTNÍ KATEGORIE OSOBNÍCH ÚDAJŮ

Pro kategorii osobních údajů, jíž se tato část diplomové práce bude věnovat, si český OchOsÚ tvoří vlastní pojmosloví a na rozdíl od unijních předpisů, které používají označení *„zvláštní kategorie osobních údajů“*, volí termín *„citlivé údaje“*.

Za citlivý údaj se dle OchOsÚ považuje *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“*, přičemž tento výčet je taxativní. Citlivé údaje jsou zvláštní kategorií osobních údajů, jejich zpracování představuje vyšší zásah do soukromí subjektu a z tohoto důvodu požadují vyšší stupeň ochrany.

Přímo jako zvláštní kategorii údajů označuje Směrnice 95/46/ES údaje, které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i údaje týkající se zdraví a sexuálního života. Obecné nařízení pak definici upřesňuje a rozšiřuje o genetické údaje a biometrické údaje

za účelem jedinečné identifikace fyzické osoby a nově výslovně stanoví, že do zvláštní kategorie osobních údajů spadají i údaje o sexuální orientaci fyzické osoby.

Je nezbytné zmínit, že OchOsÚ však již genetické a biometrické údaje mezi citlivé údaje řadil, v tomto ohledu tedy nedojde v českém právním řádu k zásadní změně. Současně však dochází k vyčlenění údajů o odsouzení za trestný čin, které jsou řazeny do nové, vlastní kategorie, upravené v čl. 10 Obecného nařízení.[37]

Unijními právními předpisy je obecně zakázáno zpracovávat osobní údaje spadající do zvláštní kategorie, mimo výslovně stanovených případů, mezi něž patří například udělení výslovného souhlasu subjektem údajů či zákonná povinnost zpracovávat takové údaje v oblasti pracovního práva či práva sociálního zabezpečení.[38]

Vyvstává otázka, zda se za citlivý údaj považuje fotografie osoby. Portrétní fotografie jistě odhaluje rasový či etnický původ osoby, může však vypovídat i o náboženství. Pracovní skupina WP 29[39], i ÚOOÚ[40] se však přiklání k závěru, že snímky nelze považovat za citlivé údaje, nejsou-li jednoznačně použity k odhalení citlivých údajů o fyzických osobách. Pokud jsou fotografie využívány k pouhému rozlišení podoby osoby ve srovnání s jinými osobami, nelze takové použití považovat za zpracování citlivých údajů.

---

[37] Osobní údaje týkající se rozsudků v trestních věcech a trestných činů lze zpracovávat pouze pod dozorem orgánu veřejné moci nebo pokud je zpracování oprávněné podle práva Evropské unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů, přičemž jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci.

[38] Čl. 9 odst. 2 Obecného nařízení.

[39] Stanovisko WP 29 č. 5/2009 k internetovým sociálním sítím.

[40] Stanovisko ÚOOÚ č. 12/2012 k použití fotografie, obrazového a zvukového záznamu osoby.

2.1.3 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Dalším pojmem neodmyslitelně spjatým s pojmem osobní údaje je jejich zpracování. OchOsÚ je definováno jako *„jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky“*. Definice dále obsahuje demonstrativní výčet operací, které lze považovat za zpracování osobních údajů.[41] Za klíčové operace z tohoto seznamu lze považovat zejména shromažďování, uchovávání, blokování a likvidaci osobních údajů.

Za zpracování osobních údajů se považuje jak zpracování automatizované, tedy zpracování prováděné s pomocí elektronických prostředků, tak zpracování neautomatizované, tedy zejména vedení papírových archivů.

Aby mohla být určitá činnost považována za zpracování osobních údajů, musí být prováděna systematicky. Za zpracování osobních údajů tak nelze považovat nahodilé shromažďování údajů, které je prováděno bez jakéhokoliv cíle, případně jejich sběr pouze pro osobní potřebu. Pokud jsou však nahodile sebraná data následně systematicky uspořádána, tato činnost se již za zpracování osobních údajů považovat bude.[42]

Definice zpracování osobních údajů v OchOsÚ sice vychází ze znění Směrnice 95/46/ES, na rozdíl od ní však přímo v definičním ustanovení stanoví, že zpracování

---

[41] § 4 OchOsÚ

„Pro účely tohoto zákona se rozumí

e) zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace,“.

[42] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 214.

musí být prováděno systematicky. Skutečnost, že se Směrnice 95/46/ES stejně jako český zákon nevztahuje na systematické zpracování osobních údajů, lze však dovodit ze znění jejího čl. 3. Ten stanoví, že v případě neautomatizovaného zpracování osobních údajů se Směrnice vztahuje pouze na takové údaje, které jsou obsaženy v rejstříku nebo do něj mají být zařazeny, tj. jsou zpracovávány v rámci určitého systému.

Za shromažďování se považuje sběr dat, která mají být následně uložena a dále zpracovávána, a to buď okamžitě, nebo později. Uchováváním se pak rozumí udržení údajů v určité podobě, ve které je bude možné nadále zpracovávat. Blokování je definováno jako omezení způsobu nebo prostředků zpracování osobních údajů na určitou dobu a konečně likvidací se rozumí fyzické zničení jejich nosiče, jejich fyzické vymazání nebo jejich trvalé vyloučení z dalších zpracování.[43] K blokování a likvidaci osobních údajů je přistupováno zejména ve chvíli, kdy pomine právní titul k jejich zpracování.

Obecné nařízení se víceméně drží zavedené definice a definuje zpracování osobních údajů jako jakoukoliv operaci či soubor operací s osobními údaji nebo soubory osobních údajů, a to automatizovaně či neautomatizovaně. I v příslušném ustanovení čl. 4 bodu 2) nalezneme demonstrativní výčet operací, které se považují za zpracování osobních údajů.[44] Obecné nařízení dále stanovuje částečné výjimky ze své působnosti. Nevztahuje se na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností. Nařízení se však vztahuje na správce

---

[43] § 4 OchOsÚ.

[44] čl. 4 bod 2) Obecného nařízení

„Pro účely tohoto nařízení se rozumí:

2) „zpracováním“ jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení;“.

nebo zpracovatele, kteří pro takové činnosti poskytují prostředky pro zpracování osobních údajů.

Zvláštním způsobem zpracování osobních údajů je tzv. profilování. Tento pojem současná evropská ani česká právní úprava nezná, byl zaveden v čl. 4 bodu 4) Obecného nařízení a rozumí se pod ním *„jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu“*.

Z výše uvedené definice vyplývá, že profilování je zpracováním, které slouží k posouzení vlastností či preferencí fyzické osoby a k vytvoření profilu takového subjektu údajů složeného z vlastností či preferencí, na jehož základě je možné předpovídat jeho chování.[45] V praxi může být profilování použito např. při zobrazování cílené reklamy subjektu údajů na základě dříve navštívených internetových stránek.

Podmínky využití profilování jsou stanoveny v čl. 22 Obecného nařízení, který vymezuje případy, v nichž může být subjekt údajů předmětem rozhodnutí založeného výhradně na profilování.

2.1.4 SUBJEKT OSOBNÍCH ÚDAJŮ

Osobou, která stojí v samém středobodu práva ochrany osobních údajů, je subjekt osobních údajů. Dle OchOsÚ se subjektem údajů rozumí fyzická osoba, k níž se údaje vztahují. Definice, kterou podává Směrnice 95/46/ES, je přesnější a uvádí, že se subjektem údajů rozumí identifikovaná nebo identifikovatelná osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či

[45] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 119.

více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity.

OchOsÚ výslovně nestanovuje, zda se jeho úprava vztahuje i na osobní údaje zemřelých osob. Touto otázkou se však zabýval ÚOOÚ ve svém stanovisku ke zpracování osobních údajů zemřelých osob.[46] V tomto stanovisku dospěl ÚOOÚ k závěru, že po úmrtí subjektu údajů pozbývají platnosti pouze ta ustanovení OchOsÚ, v nichž subjekt údajů vystupuje jako účastník občanskoprávních vztahů a naproti tomu zůstávají v platnosti ta ustanovení zákona o ochraně osobních údajů, v nichž subjekt údajů jako účastník občanskoprávních vztahů nevystupuje.

Obecné nařízení v recitálu 27 pak přímo stanoví, že se nevztahuje na osobní údaje zesnulých osob, zároveň však pravidla týkajících se zpracování osobních údajů zesnulých osob mohou stanovit samotné členské státy. Návrh zákona o zpracování osobních údajů však ve svém současném znění této možnosti nevyužil a pravidla zpracování osobních údajů zesnulých osob neupravuje.

Jak přímo ustanovení § 4 písm. d) OchOsÚ uvádí, subjektem údajů se rozumí pouze fyzická osoba. Na osoby právnické se tedy právní ochrana osobních údajů nevztahuje. Je tomu tak z důvodu, že osoby právnické jsou osobami fiktivními, které nefigurují ve sféře soukromého života a nemají tedy ani soukromí, které by bylo záhodno prostřednictvím právních předpisů z oblasti ochrany osobních údajů střežit.[47] Z povahy věci je však zřejmé, že informace vztahující se k právnické osobě mohou být osobními údaji fyzických osob, tedy např. společníků či členů statutárního orgánu právnické osoby.

---

[46] Stanovisko ÚOOÚ č. 4/2012 ke zpracování osobních údajů zemřelých osob.

[47] FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. § 4 [Vymezení pojmů]. In: KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 47.

V důsledku výše uvedeného však vyvstává otázka, jakým způsobem jsou chráněny osobní údaje fyzických osob podnikajících. U těchto osob je zřejmé, že je jejich soukromý a profesní život natolik svázán, že je obtížné rozlišit, zda se zpracovávané osobní údaje skutečně vztahují k jejich soukromí. Je tomu tak zejména z důvodu, že je velká část těchto informací veřejně dostupná. Současná česká právní úprava tuto situaci neřeší a postavení fyzických osob podnikajících výslovně neupravuje.

Skutečnost, že se fyzické osoby podnikající za subjekt údajů skutečně budou považovat, lze dovodit ze znění ustanovení § 4 písm. a) OchOsÚ, které mj. stanoví, 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. Z uvedeného vyplývá, že i osobním údajům vzniklým na základě ekonomické a podnikatelské aktivity fyzických osob je poskytována právní ochrana.

K opačnému závěru, tedy že se podnikající fyzické osoby nepovažují za subjekt osobních údajů, se přiklonil Ústavní soud v nálezu Pl. ÚS 38/02 ze dne 9. dubna 2004, v němž konstatoval následující: *„Uvedený zákon totiž vymezuje v § 1 (předmět úpravy) svoji osobní působnost tak, že se vztahuje na ochranu osobních údajů fyzických osob. Nechrání tedy osoby právnické. Pokud jde o fyzické osoby, které jsou podnikateli – a na něž se vztahuje § 11 zákona o krajích, jehož část je napadena – lze usuzovat stejně, neboť z hlediska jejich statusu je nutno za rozlišovací kritérium považovat jejich činnost podnikatelskou. Údaje o této činnosti (stejně jako v případě právnických osob) tedy – podle mínění Ústavního soudu – ochrany podle zákona č. 101/2000 Sb. nepožívají.“* Předmětný nález Ústavního soudu se však meritorně netýká OchOsÚ, z tohoto důvodu jej ÚOOÚ nepovažuje za všeobecně závazný a zastává názor, že se podnikající fyzické osoby považují za subjekt osobních údajů[48].

[48] Stanovisko ÚOOÚ č. 3/2011 k ochraně osobních údajů podnikajících fyzických osob.

Je nutné poznamenat, že Obecné nařízení rovněž nevnáší do právní úpravy osobních údajů fyzických osob podnikajících jistotu a jejich postavení taktéž výslovně neupravuje.

2.1.5 SPRÁVCE A ZPRACOVATEL

Vedle subjektu hrají zásadní roli i správce a zpracovatel osobních údajů.

Správce je OchOsÚ definován jako *„subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj“*. Definice tedy obsahuje čtyři základní prvky, které jsou pro osobu správce určující, a to a) stanovení účelu zpracování, b) určení způsobu a prostředků zpracování, c) provádění zpracování a d) odpovědnost za zpracování. V praxi je však možné, že za správce bude označena i osoba, která všechny tyto prvky nenaplňuje, tedy osoba, jež neurčila účel a prostředky zpracování, a to zejména v případě, kdy byly určeny právním předpisem, a neprovádí zpracování, jelikož jím pověřila osobu zpracovatele.[49]

Směrnice 95/46/ES i Obecné nařízení definují osoby, které mohou být správcem osobních údajů konkrétněji. Dle obou těchto předpisů může být správcem osoba fyzická, osoba právnická, orgán veřejné moci, agentura, nebo jiný subjekt.

Zásadní význam osoby správce spočívá v tom, že je osobou odpovědnou za zpracování osobních údajů.[50] I když v praxi správce nemusí naplňovat všechny znaky výše uvedené definice, z hlediska odpovědnosti je zásadní některou osobu za správce označit.

Zpracovatel, tedy dle definice OchOsÚ, Směrnice 96/45/ES i Obecného nařízení subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje, se zřizuje na základě rozhodnutí správce o přenesení svých činností

[49] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 220.

[50] Stanovisko WP 29 č. 1/2010 k pojmům správce a zpracovatel.

spojených se zpracováním osobních údajů na externí organizaci. Osoba zpracovatele osobních údajů přitom musí naplnit dva pojmové znaky. První podmínkou je, že se vzhledem ke správci jedná o samostatnou osobu, druhou pak skutečnost, že zpracovává osobní údaje pro správce, a to podle jeho pokynů. Aby byla zajištěna bezpečnost zpracování, je nutná existence smlouvy nebo jiného závazného právního aktu mezi správcem a zpracovatelem.

2.2 PRINCIPY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Ze českého zákona OchOsÚ, ze Směrnice 95/46/ES i z Obecné nařízení vyplývá, že subjekt údajů je osobou, která je oprávněným držitelem osobních údajů a může tak rozhodovat o jejich dalším využití. V důsledku toho je tedy předmětem právních předpisů na ochranu osobních údajů vymezení vztahu mezi subjektem údajů a správcem, v němž z povahy věci subjektu údajů náleží práva a správci povinnosti.[51]

Základní zásady zpracování osobních údajů představují nejvýznamnější povinnosti správce. Těmito zásadami se řídí celé právo ochrany osobních údajů, jež musí být vykládáno v souladu se základními zásadami.

Systematika zásad podle OchOsÚ vykazuje určité odlišnosti oproti systematice Směrnice 95/46/ES i Obecného nařízení. Unijní předpisy zásadám zpracování osobních údajů věnují samostatné články, konkrétně čl. 6 Směrnice 95/46/ES a čl. 5 Obecného nařízení, český OchOsÚ tyto principy upravuje v § 5, jenž shrnuje povinnosti správce.

2.2.1 ZÁKONNOST, KOREKTNOST A TRANSPARENTNOST

Směrnice 95/46/ES stanoví, že osobní údaje musí být osobní zpracovávány korektně a zákonným způsobem.[52] V OchOsÚ tuto zásadu nenalezneme explicitně vyjádřenou, částečně upravena je pouze v § 5 odst. 1 písm. c), jenž stanoví, že správce je povinen zpracovávat pouze takové osobní údaje, které získal v souladu s tímto zákonem.

---

[51] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. V Praze: C.H. Beck, 2008. Beckova edice ABC, s. 37.

[52] Čl. 6 odst. 1 písm. a) Směrnice 95/46/ES.

Princip zákonnosti je jedním z nejdůležitějších principů a nejobecnějším východiskem práva ochrany osobních údajů, z nějž vycházejí další zásady, jako je zásada účelového omezení. Princip zákonnosti zahrnuje požadavek souladu zpracování se všemi zákony, včetně souladu s ochranou osobnostních práv.[53] Zpracování osobních údajů může být považováno za zákonné pouze v případě, kdy probíhá na legitimním základě, ať již na základě souhlasu subjektu údajů, nebo jiného právního titulu.

Obecné nařízení k podmínkám zákonnosti a korektnosti přidává i výslovnou povinnost zpracování transparentním způsobem.[54] Zásada transparentnosti správce zejména zavazuje, aby subjekt údajů řádně informoval, že jsou jeho osobní údaje zpracovávány, a v jakém rozsahu se tak děje. Ačkoliv zásada transparentnosti není výslovně vyjádřena ve Směrnici 95/46/ES ani v OchOsÚ, její existenci lze snadno dovodit, jelikož oba tyto předpisy zakotvují povinnost správce podávat subjektu údajů informace o zpracování jeho osobních údajů.[55] Dalším projevem zásady transparentnosti je ustanovení § 5 odst. 1 písm. g) OchOsÚ, které stanoví správci povinnost zpracovávat osobní údaje pouze otevřeně, tedy nikoliv pod záminkou jiného účelu nebo jiné činnosti.

2.2.2 ZÁSADA ÚČELOVÉHO OMEZENÍ

Zásada účelového omezení se skládá z několika složek. Osobní údaje mohou být shromažďovány pouze pro určité, výslovně vyjádřené a legitimní účely. Osobní údaje rovněž nesmějí být dále zpracovávány způsobem, který je s vymezenými účely neslučitelný. V OchOsÚ je zásada účelového omezení vyjádřena v ustanovení § 5 odst. 1, konkrétně v písm. a), f) a h).

Povinnost stanovit účel zpracování osobních údajů je úkolem správce, nepřísluší tedy jiným osobám, zejména zpracovateli, příjemci či jiné osobě podílející se na zpracování

---

[53] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. V Praze: Wolters Kluwer, a.s., 2014, s. 140.

[54] Čl. 5 odst. 1 písm. a) Obecného nařízení.

[55] Čl. 10 a 11 Směrnice 95/46/ES, §§ 11 a 12 OchOsÚ.

osobních údajů.[56] Deklarování účelu zpracování je nutné jak v případech, kdy správce provádí zpracování na základě vlastního rozhodnutí, tak v případech, kdy zpracování probíhá na základě povinnosti stanovené zvláštním zákonem. V druhém zmíněném případě je však účel zpracování zpravidla stanoven v daném zvláštním předpisu, nebo jej lze z tohoto předpisu odvodit.

Vedle povinnosti stanovit účel zpracování osobních údajů je OchOsÚ správci stanovena i povinnost stanovit prostředky a způsob tohoto zpracování.

V praxi může dojít k situaci, kdy se s postupem času změní účel zpracování údajů a správce začne využívat již shromážděné osobní údaje k nově definovanému účelu. Takový postup je však OchOsÚ zakázán, konkrétně v ustanovení § 5 odst. 1 písm. f), jež stanoví, že správce je povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. V případě, kdy správce zjistí, že je třeba zpracovávat osobní data i k jinému účelu, je povinen stanovit nový účel, a v případě, kdy pro nové zpracování nemůže uplatnit jiný právní titul, je povinen získat rovněž souhlas subjektu údajů s tímto novým zpracováním.[57]

Dalším důležitým ustanovením, které je projevem zásady účelového omezení, je § 5 odst. 1 písm. h) OchOsÚ, jež zakazuje správci sdružovat údaje, které byly získány k rozdílným účelům. Předmětné ustanovení jde nad rámec Směrnice 95/46/ES, přičemž důvodem pro výslovné zakotvení této povinnosti správce do české právní úpravy je skutečnost, že v praxi dochází k případům, kdy kombinace údajů, které se

---

[56] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. § 5 [Práva a povinnosti správce]. In: KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 99.

[57] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. § 5 [Práva a povinnosti správce]. In: KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 99.

samostatně stojící mohou jevit jako banální, může ve výsledku v některých případech vést k výrazným dopadům do soukromé sféry osob.[58]

K problematice neoprávněného sdružování osobních údajů se v minulosti vyjadřoval i ÚOOÚ ve svém stanovisku Neoprávněné sdružování osobních údajů nezletilých.[59] ÚOOÚ se zde zabýval případem, kdy byl na základě Usnesení vlády ČR proveden výzkum životních osudů osob, které do nabytí zletilosti pobývaly ve školských zařízeních pro výkon ústavní nebo ochranné výchovy a odešly z nich do běžného života. Jádrem výzkumu bylo zjišťování míry jejich konfliktů se zákony a možná vazba mezi institucionální péčí o ně a jejich obtížným začleňováním do běžného života, případně kriminální kariérou. Došlo tedy ke shromáždění osobních údajů vypovídajících o průběhu pobytu sledovaných subjektů údajů v uvedených zařízeních, přičemž tyto informace byly následně spojeny s informacemi vypovídajícími o trestné činnosti těchto osob. K tomuto jednání však neexistoval žádný právní titul, jednalo se tedy o postup v rozporu s OchOsÚ.

2.2.3 MINIMALIZACE ÚDAJŮ

Dle písm. d) ustanovení § 5 odst. 1 OchOsÚ je správce povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Tato podmínka se týká jak hlediska potřebnosti a přiměřenosti, tak roviny časové. Zásada minimalizace údajů je vyjádřena i v unijních předpisech, konkrétně v čl. 6 odst. 1 písm. a) Směrnice 95/46/ES a v čl. 5 odst. 1 písm. c) Obecného nařízení.

Povinnost minimalizace údajů je do právních předpisů na ochranu osobních údajů zakotvena zejména z důvodu, aby byl zásah do soukromí subjektu údajů co nejmenší,

---

[58] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář*. V Praze: Wolters Kluwer, a.s., 2014, str. 144.

[59] https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=6203&n=neopravnene-sdruzovani-osobnich-udaju-nezletilych .

jedná se tedy o projev zásady proporcionality.[60] Přiměřenost se vždy váže ke stanovenému účelu zpracování, přičemž za přiměřený rozsah osobních údajů se považuje takový rozsah, který postačuje k naplnění stanoveného účelu. Mezi zpracovávanými údaji nesmí být zařazeny osobní údaje nadbytečné, které správce k naplnění stanoveného účelu nevyužije, resp. pro které bude hledat využití dodatečně.

Rozsah nezbytný pro naplnění účelu zpracování může být stanoven jednak na základě zákona, kdy je správci přesný rozsah osobních údajů stanoven právě tímto zákonem, jednak na základě vlastního rozhodnutí správce, kdy se rozsah zpracování bude odvíjet od účelu zpracování stanoveného správcem.

2.2.4 DALŠÍ ZÁSADY

Obecné nařízení a Směrnice 95/46/ES jako další zásadu zpracování osobních údajů vymezují zásadu přesnosti nebo kvality údajů.[61] V českém OchOsÚ je tato zásada vyjádřena v ustanovení § 5 odst. 1 písm. c). Tato zásada znamená, že osobní údaje musí být platné a přesné ve vztahu k účelu, pro nějž se zpracovávají. Z nepřesné lze považovat takové osobní údaje, které vykazují formální, tedy například gramatické chyby, avšak i materiálně nesprávné údaje, které vypovídají nepravdivě o skutečném stavu. ÚOOÚ v minulosti uvedl, že „*opatření směřující ke zjištění zpracování nesprávných osobních údajů jsou tak nezbytná zejména v systémech, jejichž provoz je zcela či do značné míry automatizovaný, a které jsou intenzivně využívány*“.[62]

Aby byla zajištěna přesnost osobních údajů, je správce povinen provádět v případě potřeby jejich aktualizaci. Právní předpisy však nestanoví, že je správce povinen tuto aktualizaci provádět nepřetržitě, záleží tedy na vlastním vyhodnocení správce, v jakých případech bude považovat aktualizaci osobních údajů za nezbytnou.

---

[60] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 243.

[61] Čl. 6 odst. 1 písm. d) Směrnice 95/46/ES, čl. 5 odst. 1 písm. d) Obecného nařízení.

[62] Stanovisko ÚOOÚ K problematice aktualizace zpracovávaných osobních údajů, dostupné na https://www.uoou.cz/k-problematice-aktualizace-zpracovavanych-osobnich-udaju/d-1595.

V případě, kdy správce zjistí, že zpracovává osobní údaje nepřesné, je třeba, aby je bezodkladně blokoval, doplnil nebo opravil, v krajním případě zlikvidoval. Jinými slovy, správce je povinen zajistit, aby osobní údaje opět byly přesné.

Důležitou roli pro ochranu osobních údajů hraje i zásada omezení uložení, kterou najdeme výslovně uvedenou jak v unijních právních předpisech[63], tak v českém zákoně[64], a která vyjadřuje povinnost správce uchovávat osobní údaje pouze po dobu, která je nezbytná pro jejich zpracování. Doba zpracování však nemůže být správcem stanovena jako neurčitá.[65] Po uplynutí stanovené doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědeckého či historického výzkumu a pro účely archivnictví.

Poslední zásadou, kterou výslovně mezi zásady zpracování řadí pouze Obecné nařízení[66], je zásada integrity a důvěrnosti. Projevem této zásady je povinnost správce zpracovávat osobní údaje způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Povinnost správce přijmout potřebná opatření k zabezpečení osobních údajů a konkrétní požadavky na zabezpečení osobních údajů jsou stanoveny v čl. 32 Obecného nařízení. Konkrétní povinnosti ze zásady integrity a důvěrnosti vyplývající zná však již úprava Směrnice 95/46/ES a OchOsÚ, pouze je neřadí do základních zásad.

---

[63] Čl. 5 odst. 1 písm. e) Směrnice 95/46/ES, čl. 5 odst. 1 písm. e) Obecného nařízení.

[64] § 5 odst. 1 písm. e) OchOsÚ.

[65] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. § 5 [Práva a povinnosti správce]. In: KUČEROVÁ, Alena, a kol. Zákon o ochraně osobních údajů. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 99.

[66] Čl. 5 odst. 1 písm. f) Obecného nařízení.

Unijními předpisy je dále výslovně upravena zásada odpovědnosti, kterou je správci stanovena odpovědnost za dodržení všech výše uvedených zásad, Obecné nařízení nově stanoví správci i povinnost toto dodržení doložit.[67] Nově je tedy přesunuta iniciativa na správce, jenž bude sám muset zavádět nové systémy a své postupy mít řádně zdokumentovány.[68] Jak vyplývá z čl. 24 Obecného nařízení, opatření, která musí správce k dodržení tohoto souladu přijmout, musí odpovídat míře rizika, které dané zpracování představuje.

2.3 PRÁVNÍ TITULY KE ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Právní tituly ke zpracování osobních údajů jsou zákonem uznané důvody, na jejichž základě je možné zasáhnout do práva na soukromí a ochranu osobních údajů subjektu údajů. Pokud není žádný takový právní titul dán, je zpracování osobních údajů nelegální.

Výčet právních titulů, který v současnosti podává OchOsÚ, je Obecným nařízením částečně změněn. Nově již mezi právní tituly nepatří důvody pro zpracování osobních údajů dle současného ustanovení § 5 odst. 2 písm. d), f) a g), tedy oprávněně zveřejněné údaje v souladu se zvláštním právním předpisem, poskytování osobních údajů o veřejně činné osobě nebo zpracování výlučně pro účely archivnictví. To však neznamená, že správce takové údaje nesmí zpracovávat, je však povinen je zpracovávat na základě jiného právního titulu.

2.3.1 SOUHLAS SE ZPRACOVÁNÍM

Ze systematiky OchOsÚ a uvození jeho § 5 odst. 2 vyznívá, že základním právním titulem ke zpracování osobních údajů udělení souhlasu se zpracováním. Tato úprava vyplývá z koncepce, že zásah do soukromí jednotlivce by měl být přípustný přednostně tehdy, pokud s tím daný člověk souhlasí, bez souhlasu subjektu je možné

[67] Čl. 6 odst. 2 Směrnice 95/46/ES, čl. 5 odst. 2 Obecného nařízení.

[68] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 119.

osobní údaje zpracovávat teprve tehdy, kdy právo jednotlivce na ochranu soukromí je převáženo legitimním právním zájmem jiného subjektu.[69]

Řazení, které OchOsÚ provádí, však není zcela správné, jedná se o projev nepřesné transpozice Směrnice 95/46/ES, jež na rozdíl od českého zákona žádný právní titul nevytyčuje nad ostatní všechny právní tituly ke zpracování řadí na stejnou úroveň.[70] Stejně tak Obecné nařízení považuje všechny právní tituly za rovnocenné. Pro vyjádření souhlasu stanoví v čl. 7 několik nových podmínek, s jeho aplikací tak dojde k částečným změnám.

Podmínky pro udělení souhlasu jsou částečně stanovené již v čl. 4 Obecného nařízení, z něhož vyplývá, že souhlas musí být svobodný, konkrétní, informovaný a jednoznačný, přičemž subjekt jím dává prohlášením či jiným zjevným potvrzením svolení ke zpracování osobních údajů. Obecné nařízení tak rozšiřuje podmínky stanovené současnými předpisy, jež pouze vyžadují, aby byl souhlas svobodný a vědomý, přičemž Směrnice 95/46/ES přidává ještě podmínku výslovnosti souhlasu.

Vyjádření souhlasu nesmí být důsledkem zastrašování, nátlaku, či předstírání nepravdivých skutečností, takové vyjádření se považuje za nesvobodné. Obecné nařízení samo vymezuje několik situací, v nichž bude udělení souhlasu nově považováno za nesvobodné, přičemž tímto výčtem rozšiřuje současné pojetí nesvobodného jednání subjektu údajů.

Prvním z těchto případů je udělení souhlasu v situaci, kdy mezi subjektem údajů a správcem existuje nerovnováha, zejména pokud je správce orgánem veřejné moci. Dalším příkladem může být případ, kdy subjekt údajů nemá možnost vyjádřit souhlas pouze s některými operacemi zpracování, přestože je to v daném případě možné a

---

[69] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. § 5 [Práva a povinnosti správce]. In: KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 99.

[70] Čl. 7 Směrnice 95/46/ES.

vhodné. Je nutné podotknout, že obě tyto situace vyjmenovává Obecné nařízení ve svém recitálu č. 43. Poslední příklad nesvobodně uděleného souhlasu je upraven v čl. 7 odst. 4, tedy přímo ve znění Obecného nařízení a jedná se o případ, kdy je plnění smlouvy, včetně poskytnutí služby, učiněno závislým na souhlasu, i když to pro plnění není nezbytné.

Již dle současné právní úpravy je správce povinen doložit, že subjekt údajů souhlas udělil, přičemž tato povinnost správci neodpadne ani s účinností Obecného nařízení. Ačkoliv právní předpisy výslovně nestanoví, že souhlas musí být udělen písemně, lze snadno dovodit, že pro umožnění pozdějšího doložení udělení souhlasu správci zpravidla budou nuceni přikročit k vyžadování písemného souhlasu. Ze záznamů správce by mělo být patrné, že správce splnil veškeré podmínky Obecným nařízením stanovené, tedy informace o tom, kdo souhlas udělil, kdy se tomu tak stalo, o jakých skutečnostech byl subjekt údajů před udělením souhlasu informován, jak byl souhlas udělen, případně údaj o tom, zda byl souhlas odvolán.[71]

Pokud je souhlas udělován písemným prohlášením, které souvisí i s jinými skutečnostmi, musí být dle Obecného nařízení subjektu údajů zřejmé, že souhlas se zpracováním osobních údajů dává a v jakém rozsahu. Prohlášení o souhlasu by mělo být poskytnuto ve srozumitelném a snadno přístupném znění za použití jasného a jednoduchého jazyka a nemělo by obsahovat nepřiměřené podmínky.[72] Žádost o vyjádření souhlasu by měla být správcem předložena způsobem, který je od zmíněných jiných skutečností jasně odlišitelný. V praxi to znamená, že bude vyloučeno umisťovat souhlas se zpracováním do VOP a adhezních (formulářových) smluv, jejich současné znění a způsob vyžadování souhlasu se zpracováním tedy budou správci nuceni upravit.[73]

---

[71] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 149.

[72] Recitál č. 42 Obecného nařízení.

[73] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 151.

Subjekt údajů je oprávněn souhlas se zpracováním kdykoliv odvolat. Odvoláním souhlasu se zpracováním zaniká právní titul správce pro zpracování a není tak dále oprávněn osobní údaje zpracovávat. Dle Obecného nařízení subjektu údajů vzniká po odvolání souhlasu také právo na výmaz (tzv. „právo být zapomenut“).[74] Odvolat souhlas přitom dle čl. 7 odst. 4 Obecného nařízení musí být stejně snadné jako jej poskytnout. Je ovšem namístě zdůraznit, že se nejedná o nové oprávnění subjektu údajů, neboť tomu bylo toto právo přiznáno i před jeho výslovným zakotvením, a to na základě práva každého činit to, co není zákonem zakázáno.[75]

Možnosti subjektu osobních údajů odvolat souhlas se zpracováním osobních údajů se dotýká rovněž obč. zák. v jeho § 87 odst. 1. Dle tohoto ustanovení může ten, kdo svolil k použití písemnosti osobní povahy, podobizny nebo zvukového či obrazového záznamu týkajícího se jeho osoby nebo jeho projevů osobní povahy, svolení odvolat, třebaže je udělil na určitou dobu. Předmětné ustanovení tedy obecně umožnuje odvolání předchozího souhlasu k použití materiálů, které mohou rovněž obsahovat osobní údaje za předpokladu, že obsahují informace o subjektu údajů a ten je na jejich základě určený nebo určitelný.

Možnost odvolání souhlasu k použití výše uvedeného okruhu materiálů osobní povahy ovšem není bezbřehá. Limitaci obsahuje § 87 odst. 2 obč. zák., podle něhož v případech, kdy osoba udělila svolení na určitou dobu, a toto svolení odvolá, aniž by takové odvolání odůvodňovala podstatná změna okolností nebo jiný rozumný důvod, má osoba, jíž byl souhlas udělen, právo na náhradu škody vzniklé v důsledku takového odvolání. Smyslem daného ustanovení je ochrana legitimního očekávání osoby, jíž byl souhlas udělen ohledně trvání souhlasu uděleného na dobu určitou. Taková osoba přitom mohla vynaložit množství peněžních či jiných prostředků za účelem udělení

[74] Čl. 17 Obecného nařízení.

[75] Stanovisko ÚOOÚ k problematice odvolatelnosti souhlasu se zpracováním osobních údajů https://www.uoou.cz/k-problematice-odvolatelnosti-souhlasu-se-zpracovanim-osobnich-udaju/d-10891 .

souhlasu s použitím výše uvedeného materiálu osobní povahy, kdy taková činnost měla povahu hospodářské investice. Pokud by legitimní očekávání ohledně trvání souhlasu nebylo zajištěno ustanovením § 87 odst. 2 obč. zák, vyvstalo by pro uživatele materiálů osobní povahy značné riziko pro jejich investici, a takový stav by mohl vést až podstatnému úbytku či ochromení průmyslových odvětví založených na používání materiálů osobní povahy.[76] Odvolání souhlasu nemá být v žádném případě nikomu na újmu.[77] Dané ustanovení ale v žádném případě nelze vykládat v tom smyslu, že by obsahovalo zákaz odvolání souhlasu. Osoba poskytnuvší souhlas má v každém případě plné právo souhlas odvolat, pokud se ovšem nebude jednat o případ uvedený v předmětném ustanovení, musí počítat s možností povinnosti k náhradě škody způsobené předčasným odvoláním souhlasu.[78]

V případech, kdy použití materiálů osobní povahy naplní podstatu zpracování osobních údajů, bude na tyto případy nutno aplikovat vedle obecné právní úpravy obsažené v obč. zák. rovněž úpravu týkající se ochrany osobních údajů.

Rozlišit, v jakých případech se uplatní pouze obecná právní úprava ochrany osobnosti dle obč. zák. a na jaké situace už dopadá zvláštní ochrana osobních údajů, je ovšem značně problematické. Pokud bychom přijali závěr, že se skutečně jedná o dvě rozdílné oblasti právní úpravy, bylo by nutné uplatnit zásadu aplikační přednosti *lex specialis derogati legi generali*[79]. V takovém případě by OchOsÚ, potažmo evropská úprava ochrany osobních údajů, měla jako speciální právní předpis aplikační přednost před obecnou právní úpravou obč. zák.

---

[76] Např. filmový průmysl.

[77] TŮMA, Pavel. § 87 [Ochrana písemností osobní povahy, podobizen a záznamů člověka]. In:, LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2014, s. 524.

[78] TŮMA, Pavel. § 87 [Ochrana písemností osobní povahy, podobizen a záznamů člověka]. In:, LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1−654)*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2014, s. 524.

[79] Zvláštní úprava má přednost před normou obecnou, která se uplatní jen tam, kde zvláštní právní předpis věc sám neupravuje.

Zbývá tedy nastínit, na jaké případy se aplikuje obecná právní úprava a na jaké úprava speciální. Úprava práva ochrany osobních údajů se uplatní v případech, kdy informace ohledně určité či určitelné fyzické osoby budou zpracovávány ve smyslu OchOsÚ, resp. Obecného nařízení. Pro takové zpracování je typická systematičnost a určitý účel. Pokud používání poskytnutých údajů svou kvalitou nedosáhne úrovně samotného zpracování osobních údajů, nebudou na něj pravidla vyplývající z práva na ochranu osobních údajů dopadat. Takovým použitím mohou být případy, kdy projevy osobní povahy nejsou zpracovány systematicky, ale jedná se spíše o použití jednorázové či nahodilé. V takových případech se uplatní obecná právní úprava ochrany dle obč. zák.[80]

2.3.2 PLNĚNÍ SMLOUVY A PLNĚNÍ PRÁVNÍ POVINNOSTI

Dalším právním titulem pro zpracování osobních údajů je jeho nezbytnost pro plnění smlouvy, přičemž pod pojmem plnění smlouvy lze rozumět jak její sjednávání, tak plnění již uzavřené smlouvy a její změny.[81] Správce je vždy povinen stanovit účel dané smlouvy a zpracovávat osobní údaje pouze k jeho dosažení.

V rámci pracovněprávních vztahů lze za příklad zpracování na smluvním základě uvést zpracování osobních údajů potencionálního zaměstnance, který se u zaměstnavatele účastní výběrového řízení či pohovoru. K samotnému uzavření pracovní smlouvy s konkrétním subjektem osobních údajů přitom v budoucnu nemusí nutně dojít. Ke vzniku titulu k zpracování osobních údajů postačí, pokud zaměstnavatel má skutečně má v úmyslu předmětné pracovní místo obsadit a za tímto účelem zpracovává osobní údaje uchazečů o něj. Právní titul ke zpracování by tak zjevně nemohl vzniknout např. za situace, kdy určitá osoba předstírá zájem o přijetí nových zaměstnanců a za tímto účelem shromažďuje osobní údaje zájemců o pracovní místo, kdy skutečným záměrem takto jednající osoby je zpracování osobních údajů

[80] NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. Právní rozhledy. 2012, č. 13-14, s. 505-509.

[81] Čl. 7 písm. b) Směrnice 95/46/ES, § 5 odst. 2 písm. b) OchOsÚ, čl. 6 odst. 1 písm. b) Obecného nařízení.

uchazečů za účelem reklamy. Výše předestřenou situaci by pak bylo nutné posoudit jako zpracování osobních údajů bez právního titulu, tedy jako zpracování neoprávněné. Zároveň je nutné zmínit, potencionální zaměstnavatel může zpracovávat pouze takové *„údaje, které jsou nutné ke svobodnému a vážnému rozhodnutí zaměstnavatele o tom, že s konkrétním zaměstnancem uzavře pracovní poměr“*.[82]

Dále pak může ke zpracování osobních údajů správci vzniknout právní povinnost přímo ze zákona, nebo na základě zákona v důsledku právní skutečnosti nebo z rozhodnutí orgánu veřejné moci.[83] Obecným nařízením je nově stanovena podmínka, že taková právní povinnost musí vyplývat z práva členského státu nebo EU.

Právním předpisem musí být stanovena povinnost a nikoliv oprávnění, jedná se tedy o případy, kdy správce nemá na výběr, zda tuto povinnost splní či ne. Čl. 6 odst. 3 Obecného nařízení dále stanoví určité náležitosti právního základu, z nějž zpracování vychází. Ten musí obsahovat obecné podmínky, kterými se řídí zákonnost zpracování, typ osobních údajů, které mají být zpracovány, určení dotčených subjektů údajů, subjektů, kterým lze osobní údaje poskytnout, apod. Zároveň je nezbytné, aby právní základ splňoval cíl veřejného zájmu a byl přiměřený sledovanému cíli.

Příkladem zpracování osobních údajů za účelem plnění právní povinnosti z oblasti pracovněprávních vztahů může být povinnost zaměstnavatele vést evidenci pracovní doby zaměstnanců dle § 96 ZPr či povinnost vést knihu úrazů ve smyslu § 105 ZPr. Zaměstnavatel má dále zákonem uloženou povinnost zpracovávat osobní údaje svých zaměstnanců pro účely daňové a pro účely sociálního zabezpečení. V daňové oblasti zaměstnavateli povinnost zpracovávat osobní údaje zaměstnanců vyplývá např. z § 38j zákona č. 586/1992 Sb., o daních z příjmů, kde jsou uvedeny povinné náležitosti tzv. mzdového listu. Úpravu povinného zpracování osobních údajů dále pro účely

[82] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 377.

[83] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 264.

sociálního zabezpečení obsahuje zejména zákon č. 582/1991 Sb., o organizaci sociálního zabezpečení, zákon č. 187/2006 Sb., o nemocenském pojištění či zákon č. 155/1995 Sb., o důchodovém pojištění.

Pro zpracování osobních údajů na základě povinností vyplývající zpracovateli ze zákona je typické, že jde o povinnosti kogentní povahy a nelze se od nich proto v důsledku dohody mezi zpracovatelem a subjektem osobních údajů odchýlit. Souhrnně pak lze oblast zpracování osobních údajů, která se realizuje na základě kogentních právní předpisů a která je svou povahou obligatorní, označit za zpracování osobních údajů pro účely personální a mzdové agendy, kdy se neuplatní oznamovací povinnost vůči ÚOOÚ.[84]

2.3.3 OCHRANA ŽIVOTNĚ DŮLEŽITÝCH ZÁJMŮ

Správce má možnost zpracovávat osobní údaje i v případě, kdy je to nezbytně třeba k ochraně životně důležitých zájmů.[85] Pojem ohrožení životně důležitých zájmů není českými ani unijními právními předpisy definován, lze pod ním však rozumět takový stav, kdy by v důsledku nezískání osobních údajů byl reálně ohrožen subjekt údajů způsobem, který by mohl mít dopady na jeho život či zdraví nebo jiný zájem, který by byl subjektem osobních údajů vnímán jako životně důležitý. Za životně důležité zájmy lze rovněž považovat humanitární účely, včetně monitorování epidemií a jejich šíření nebo naléhavé humanitární situace, zejména v případech přírodních a jiných katastrof.[86]

Dle OchOsÚ a Směrnice 95/46/ES je pro použití tohoto právního titulu nezbytné, aby byl ohrožen životně důležitý zájem samotného subjektu údajů. Obecné nařízení od této podmínky upouští a nově tak lze na základě titulu ochrany ohrožení životně důležitých zájmů zpracovávat osobní údaje i takových subjektů údajů, jejichž životně důležitý

---

[84] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 174.

[85] Čl. 7 písm. d) Směrnice 95/46/ES, § 5 odst. 2 písm. c) OchOsÚ, čl. 6 odst. 1 písm. d) Obecného nařízení.

[86] Recitál č. 46 Obecného nařízení.

zájem není v danou chvíli přímo ohrožen, je však ohrožen životně důležitý zájem jiné osoby.

OchOsÚ podmiňuje zpracování osobních údajů z důvodu ochrany životně důležitých zájmů podmínkou, aby byl bez zbytečného odkladu získán souhlas subjektu údajů. Pokud jej subjekt údajů neudělí, je správce povinen ukončit zpracování a osobní údaje zlikvidovat. Směrnice 95/46/ES však natolik přísná není a dle jejího znění tak není nutné dodatečný souhlas subjektu údajů získávat. Obecné nařízení se v tomto ohledu přiklání ke znění Směrnice 95/46/ES a rovněž nepodmiňuje použití tohoto právního titulu dodatečným získáním souhlasu. Vzhledem k povaze Obecného nařízení, jenž je přímo aplikovatelné, tak dojde k částečnému uvolnění dosavadní právní úpravy.

Ačkoliv je právní titul zpracování osobních údajů z důvodu ohrožení životně důležitých zájmů fyzické osoby rovnocenný s ostatními právními tituly zpracování, takové zpracování by mělo probíhat pouze v případě, kdy nemůže být založeno na jiném základě.[87]

2.3.4 OCHRANA OPRÁVNĚNÝCH ZÁJMŮ SPRÁVCE A TŘETÍCH OSOB

Dalším právním titulem pro zpracování osobních údajů je zpracování nezbytné pro účely ochrany práv a právem chráněných zájmů správce, příjemce, nebo jiné dotčené osoby.[88] Takové zpracování je však správce oprávněn provést pouze v případě, kdy takové zpracování není v rozporu s právem subjektu údajů na ochranu jeho soukromého nebo osobního života. Z tohoto vymezení vyplývá, že je správce vždy před zahájením zpracování povinen provést posouzení, zda je zpracování skutečně nezbytné, a zda v daném konkrétním případě převažují jeho oprávněné zájmy nad právy subjektu údajů.

[87] Recitál č. 46 Obecného nařízení.

[88] Čl. 7 písm. f) Směrnice 95/46/ES, § 5 odst. 2 písm. e) OchOsÚ, čl. 6 odst. 1 písm. f) Obecného nařízení.

Současné znění OchOsÚ a Směrnice 95/46/ES je do jisté míry omezující v tom, že jako podmínku stanoví ochranu práv a právem chráněných zájmů správce, příjemce či jiné dotčené osoby. Není tedy možné, aby si správce určil vlastní oprávněný zájem a osobní údaje zpracovával na jeho základě a je nezbytné, aby se jednalo o právním řádem uznaný zájem správce. V praxi tak bude tento právní titul využíván často při monitorování zaměstnanců prostřednictvím kamerového systému, kdy zaměstnavatel zásah do práv svých zaměstnanců povětšinou legitimizuje svým zájmem na ochraně majetku.

Vzhledem ke skutečnosti, že zaměstnanec při výkonu závislé práce užívá převážně prostředky nikoli vlastní, avšak prostředky nacházející se ve vlastnictví zaměstnavatele, který má oprávněný zájem na ochraně svého majetku, upravil zákonodárce v oblasti pracovněprávních vztahů podrobněji možnost zaměstnavatele zpracovávat osobní údaje zaměstnanců vzhledem k ochraně svých výrobních a pracovních prostředků. Tato právní úprava vychází ze samotné podstaty závislé práce, která má být konána na náklady zaměstnavatele, a použití prostředků zaměstnavatele se jeví jako zcela logický požadavek. Zaměstnavatel jakožto vlastník předmětných pracovních prostředků má ústavně zaručené právo na ochranu svého majetku. Ustanovení § 316 odst. 1 ZPr proto obsahuje zákaz zaměstnanců užívat bez souhlasu zaměstnavatele prostředky ve vlastnictví zaměstnavatele pro osobní potřebu. Dodržování tohoto zákazu je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.[89]

Právní úprava obsažená v ZPr je přitom vůči OchOsÚ úpravou speciální, která se uplatní výlučně v pracovněprávních vztazích.[90] Zákonodárce tak přímo pojmenovává a konkretizuje oprávněný zájem zaměstnavatele coby správce osobních údajů na zpracování osobních údajů a stanoví jeho podmínky.

[89] § 316 odst. 1 ZPr.

[90] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 399.

Výše uvedené ovšem v žádném případě neznamená, že by byl zaměstnavatel zproštěn povinnosti provést test proporcionality konkrétního zásahu do práv subjektu osobních údajů, a zpracování osobních údajů je povinen vykonávat s ohledem na skutkové okolnosti konkrétního případu.[91]

Obecné nařízení již používá pojem oprávněné zájmy správce, umožňuje tedy, aby si subjektivní oprávněný zájem stanovil správce sám. Dle recitálu 47 Obecného nařízení se v praxi může jednat zejména o potřeby marketingu či snahu o zamezení podvodům. Jako další příklady lze uvést vymáhání právních nároků, IT a síťová bezpečnost, nebo vědecký výzkum.[92] Toto nové oprávnění však pro správce znamená, že je v rámci posuzování zamýšleného zpracování povinen posoudit, zda je jím stanovený zájem skutečně oprávněný.

Obecné nařízení zužuje okruh osob, jež budou oprávněny tento právní titul použít, přičemž nově ho již nesmějí využívat orgány veřejné moci při plnění jejich úkolů. Orgány veřejné moci tak budou povinny využívat při plnění svých úkolů jiné právní tituly, nejčastěji zpracování nezbytné pro plnění právní povinnosti nebo nový titul zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu.

2.3.5 ÚKOL VE VEŘEJNÉM ZÁJMU NEBO VÝKON VEŘEJNÉ MOCI

Zpracování osobních údajů nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci je zcela novým právním titulem, jenž zavádí Obecné nařízení v čl. 6 odst. 1 písm. e). Ačkoliv je tento právní titul obsažen ve Směrnici 95/46/ES[93], v OchOsÚ chybí, orgány veřejné správy tak v současnosti využívají pouze titul plnění právní povinnosti.

---

[91] MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer Česká republika, 2013, s. 400.

[92] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 119.

[93] Čl. 7 písm. e) Směrnice 95/46/ES.

Tento právní titul tedy slouží zejména pro zpracování osobních údajů orgány veřejné moci, ale užívat jej mohou i soukromé osoby, které jsou pověřené výkonem veřejné moci. Na rozdíl od právního titulu plnění právní povinnosti se tento právní titul nevztahuje pouze na případy, kdy je správci přikázáno, aby zpracování osobních údajů prováděl. Tento právní titul však nezavádí možnost orgánů veřejné moci zpracovávat osobní údaje libovolně, vždy se tak musí dít při plnění nějakého úkolu.

OchOsÚ upravuje další tři právní tituly ke zpracování osobních údajů, které již Obecné nařízení nezná, konkrétně jsou upravena v ustanovení § 5 odst. 2 písm. d), f) a g). S nabytím účinnosti Obecného nařízení tak správci nebudou nadále oprávněni zpracovávat osobní údaje na základě těchto právních titulů a budou zpracování nuceni opřít o některý z výše vyjmenovaných titulů.

Prvním z nich je oprávněné zveřejnění osobních údajů v souladu se zvláštním právním předpisem, za současné nutnosti přihlížet k ochraně soukromého a osobního života subjektu údajů. Správce je tedy vždy při využití tohoto právního titulu povinen provést posouzení, zda je jím prováděné zpracování přiměřené. Příkladem takových osobních údajů mohou být údaje zveřejněné podle zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání, nebo údaje zveřejněné ve veřejné části obchodního rejstříku, či jiných veřejných rejstřících a veřejných seznamech.

Ustanovení § 5 odst. 2 písm. f) OchOsÚ opravňuje správce ke zpracování osobních údajů o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení. Takové zpracování se týká veřejné či úřední činnosti dané osoby a zpravidla nezasahuje do osobního a soukromého života subjektu údajů. Je nutné podotknout, že toto ustanovení se týká pouze poskytovaní osobních údajů, nikoliv jejich dalšího zpracování, k němuž je správce povinen využít jiný právní titul.

Posledním právním titulem, na jehož základě je možné zpracovávat osobní údaje dle OchOsÚ a Obecným nařízením již výslovně upraven není, je zpracování osobních údajů výlučně pro účely archivnictví podle zvláštního zákona. Tento právní titul není

upraven ani ve Směrnicí 95/46/ES, jedná se však o projev toho, že jej unijní předpisy podřazují pod obecné zmocnění ke zpracování osobních údajů z důvodu plnění právních povinností.[94]

[94] KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. § 5 [Práva a povinnosti správce]. In: KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 99.

III. POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

3.1 PŮVOD INSTITUTU POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

Pověřenec pro ochranu osobních údajů (dále jen „pověřenec“) je osobou s odbornými znalostmi v oblasti právních předpisů a postupů týkajících se ochrany osobních údajů, která by měla být nápomocna správci při plnění jeho povinností souvisejících se zpracováním.[95]

Koncept pověřence je pro řadu členských států Evropské unie zcela nový, nejedná se však o institut, který by byl zaveden až samotným Obecným nařízením. Ačkoliv Směrnice 95/46/ES neukládala správcům povinnost pověřence jmenovat, v několika členských státech Evropské unie se tento institut přesto rozvinul, konkrétně v Německu, Francii, Maďarsku, Slovinsku či Polsku. V některých dalších členských státech, jako je např. Slovensko, pak správci nemají povinnost pověřence jmenovat, avšak může jim to přinést některé výhody.[96]

3.2 POVINNOST JMENOVAT POVĚŘENCE

V Obecném nařízení jsou případy, kdy je správce a zpracovatel povinen jmenovat pověřence, upraveny v čl. 37 odst. 1, a to následovně:

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
b) hlavní činnosti správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů; nebo
c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.

---

[95] Recitál č. 97 Obecného nařízení.

[96] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 332.

Jednotlivé případy povinného jmenování pověřence budou detailně rozebrány níže.

3.2.1 VEŘEJNÝ ORGÁN NEBO VEŘEJNÝ SUBJEKT

Pojem orgánu veřejné moci či veřejného subjektu není Obecným nařízením definován. WP29 sice označuje za orgány veřejné moci nebo veřejné subjekty všechny národní, regionální a místní úřady a další subjekty řídící se národním právem, zmiňuje však, že tento pojem by měl být definován národním právem.[97]

Je však nutné zmínit, že žádný v současnosti platný český právní předpis nepodává definici orgánu veřejné moci. Do doby, než bude tato otázka posouzena Soudním dvorem Evropské unie, který bude v konečném důsledku o sporných otázkách aplikace Obecného nařízení rozhodovat, bude nutné využít výklad tohoto pojmu, jak jej podává český Ústavní soud.[98]

Pojem veřejný subjekt však není o mnoho jasnější. V praxi se vyskytují případy, kdy zpracování v rámci úkolu ve veřejném zájmu a výkonu veřejné moci neprovádí přímo stát, veřejnoprávní korporace nebo veřejné ústavy a podniky, nýbrž jiné fyzické nebo právnické osoby soukromého práva. Mohou tak činit na základě různých právních titulů v následujících případech:

---

[97] WP29 Guidelines on Data Protection Officers ('DPOs') (*překlad vlastní*).

[98] Např. nález Ústavního soudu ze dne 10. listopadu 1998, sp. zn. I. ÚS 229/98: *„(…)moc, která autoritativně rozhoduje o právech a povinnostech subjektů, ať již přímo nebo zprostředkovaně. Subjekt, o jehož právech nebo povinnostech rozhoduje orgán veřejné moci, není s ním v rovnoprávném postavení, a obsah rozhodnutí tohoto orgánu nezávisí od vůle subjektu. Veřejnou moc vykonává stát především prostřednictvím orgánů moci zákonodárné, výkonné a soudní, a za určitých podmínek ji může vykonávat i prostřednictvím dalších subjektů. Kritériem pro určení, zda i jiný subjekt jedná jako orgán veřejné moci, je skutečnost, zda konkrétní subjekt rozhoduje o právech a povinnostech jiných osob a tato rozhodnutí jsou státní mocí vynutitelná nebo zda může stát do těchto práv a povinností zasahovat. Orgánem v právním slova smyslu je právnická osoba, vykonávající svou činnost jako povinnost nebo kompetenci a je zřízena k trvalému a opakujícímu se výkonu činnosti(…)“.*

- zákonem nebo rozhodnutím státního orgánu na ně byla přenesena určitá působnost a pravomoc,
- na základě uzavření smlouvy (zejména veřejnoprávní) o plnění některých veřejných úkolů s jiným dosavadním veřejným subjektem,
- byla založena nová právnická osoba soukromého práva za účelem dosahování obecně prospěšných cílů (nadace, nadační fondy a obecně prospěšné právnické osoby).[99]

Postavení subjektů údajů těchto správců je obdobné jako postavení subjektů, jejichž osobní údaje zpracovává orgán veřejné moci nebo veřejný subjekt. Dle WP29 však tyto subjekty nejsou povinny pověřence jmenovat.[100] K obdobnému závěru zřejmě došli i tvůrci návrhu zákona o zpracování osobních údajů. Ten definuje veřejný subjekt jako orgán zřízený zákonem nebo na základě zákona v oblasti práva veřejného, který plní zákonem stanovené úkoly ve veřejném zájmu.[101]

Ustanovení čl. 37 odst. 1 písm. a) Obecného nařízení obsahuje výjimku pro soudy jednající v rámci svých soudních pravomocí. Pro tato zpracování tedy soud nebude povinen pověřence jmenovat. Zpracování, které však nebude soudy prováděno v rámci jejich soudních pravomocí, tedy například sledování budovy soudu kamerovým systémem, však pod tuto výjimku nespadá a soud pro ně bude povinen pověřence jmenovat.[102]

3.2.2 HLAVNÍ ČINNOST SPRÁVCE A ZPRACOVATELE

Další kategorii povinných správců a zpracovatelů tvoří ti, jejichž hlavní činnosti spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým

---

[99] KOPECKÝ, Martin. In: HENDRYCH, Dušan a kol. Správní právo. Obecná část. 9. Vydání. Praha: C.H. Beck, 2016, s. 72.

[100] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

[101] § 13 návrhu zákona o zpracování osobních údajů.

[102] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 119.

účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů. Toto vymezení povinného subjektu je provedeno s pomocí několika pojmů, které Obecným nařízením nejsou přímo definovány. Domnívám se, že v praxi bude toto ustanovení činit značné výkladové problémy a řadě správců nebude zřejmé, zda jsou pověřence povinni jmenovat či nikoliv.

Jak z výše uvedeného vyplývá, pro určení, zda správce nebo zpracovatel naplňuje podmínky stanovené ustanovením čl. 37 odst. 1 písm. b), je nejprve nutné provést definici několika pojmů, konkrétně se jedná o pojmy hlavní činnost, rozsáhlé zpracování a pravidelné a systematické monitorování.

Určité vodítko pro vymezení pojmu hlavní činnost podává recitál č. 97 Obecného nařízení, jenž stanoví, že v soukromém sektoru souvisejí hlavní činnosti správce s jeho základními činnostmi a nevztahují se na zpracování osobních údajů jakožto pomocnou činnost. Jedná se o hlavní aktivity, které jsou nezbytné k dosažení cílů správce nebo zpracovatele a tvoří jejich nedílnou část. Jinými slovy, v případě, kdy by správce nebo zpracovatel takové zpracování osobních údajů neprováděl, nebyl by schopen plně naplňovat účel své existence.

Jako příklad hlavní činnosti správce nebo zpracovatele může sloužit činnost bezpečnostní agentury, jež provozuje kamerové systémy a vykonává dohled nad záběry z nich. Za hlavní činnost lze zcela jistě považovat i činnost provozovatelů sociálních sítí při jejich spravování. Jiným příkladem může být i provádění identifikace a kontroly klientů správci[103], kteří jsou dle zákona č. 253/2008 Sb.,

[103] Identifikace klienta pro účely AML zákona spočívá ve zjištění identifikačních údajů, jež tvoří všechna jména a příjmení, rodné číslo, a nebylo-li přiděleno, datum narození, dále místo narození, pohlaví, trvalý nebo jiný pobyt a státní občanství; jde-li o podnikající fyzickou osobu, též její obchodní firma, odlišující dodatek nebo další označení, místo podnikání a identifikační číslo osoby.
Kontrola klienta zahrnuje následující kroky:

a) získání informací o účelu a zamýšlené povaze obchodu nebo obchodního vztahu,

o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (dále jen „AML zákon“), osobami povinnými pro provádění této identifikace a kontroly, tedy např. finanční instituce či provozovatelé hazardních her. Tyto povinné osoby nejsou oprávněny vykonávat určité činnosti, zejména se svými klienty uzavírat obchodní vztahy nebo obchody s hodnotou přesahující částku 1 000 EUR, aniž by nejprve identifikaci a kontrolu klienta provedly, bez tohoto tedy nemohou např. provést směnu cizích měn, případně umožnit účast na hazardní hře.

Aby správci či zpracovateli vznikla povinnost jmenovat pověřence na základě tohoto ustanovení, je dále nutné, aby prováděl rozsáhlé zpracování. Otázku, jaké zpracování se považuje za rozsáhlé, zodpovídá Obecné nařízení pouze částečně, a to v recitálu 91, jež se však týká posouzení vlivu na ochranu osobních údajů a dle nějž jde o *„rozsáhlé operace zpracování, jež mají sloužit ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů a u nichž je pravděpodobné, že budou představovat vysoké riziko“*. Stejný recitál dále stanoví, že *„zpracování osobních údajů by nemělo být považováno za zpracování velkého rozsahu, pokud se jedná o zpracování osobních údajů pacientů nebo klientů jednotlivými lékaři, zdravotníky nebo právníky“*.

Ani tento výčet zpracování považovaných za rozsáhlé však není zcela konkrétní a řadě správců vznikne nejistota, zda skutečně spadají do kategorie povinných osob. Řešení nastalé situace nenapomáhá ani WP29, jež ve svém stanovisku k pověřencům[104] sama

b) průběžné sledování obchodního vztahu včetně přezkoumávání obchodů prováděných v průběhu daného vztahu za účelem zjištění, zda obchody jsou v souladu s tím, co je povinné osobě známo o klientovi a jeho podnikatelském a rizikovém profilu,
c) přezkoumávání zdrojů peněžních prostředků nebo jiného majetku, kterého se obchod nebo obchodní vztah týká, a
d) v rámci obchodního vztahu s politicky exponovanou osobou též přiměřená opatření ke zjištění původu jejího majetku.

[104] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

říká, že není možné uvést žádné přesné a pro všechny situace použitelné číslo či jiný údaj, na jehož základě by bylo možné jednoznačně určit rozsáhlost zpracování. Vždy však doporučuje vzít při určování rozsáhlosti v úvahu tyto faktory:

- počet dotčených subjektů – vyjádřený buď konkrétním číslem, nebo podílem na relevantní populaci,
- objem dat a/nebo rozsah různých datových položek,
- doba trvání nebo nepřetržitost zpracování,
- územní rozsah zpracování.

Pokud se budeme držet příkladů uvedených výše u definice hlavní činnosti správce a zpracovatele, je vhodné zmínit, že ve věci rozsáhlosti není možné provádět generalizaci a její určení se vždy bude odvíjet od povahy zpracování konkrétního správce či zpracovatele. Co se týče finančních institucí, za rozsáhlé zpracování se téměř jistě bude považovat zpracování osobních údajů v rámci obchodní činnosti banky, zároveň však za rozsáhlé zpracování nelze považovat provádění identifikace a kontroly klientů prováděné směnárnou, která disponuje pouze jednou pobočkou v menším městě. Stejně tak lze za rozsáhlé zpracování považovat sledování kamerovým systémem, které bezpečnostní agentura zabezpečuje pro několik obchodních středisek v hlavním městě Praze, nebo provozovatele největších sociálních sítí jako jsou např. Facebook nebo Instagram, za rozsáhlé však nelze považovat provozování kamerového systému, který snímá pouze recepci menší advokátní kanceláře.

Poslední podmínkou, při jejímž splnění je správce nebo zpracovatel povinen pověřence jmenovat, je provádění pravidelného a systematického monitorování. Stejně jako v předchozích případech, WP29 podává určitá vodítka, jimiž by se správci měli řídit při určování, zda podmínku pravidelného a systematického monitorování naplňují.

Za pravidelné považuje WP29 takové zpracování, které probíhá průběžně nebo v pravidelných intervalech, které se stále, případně po určitou dobu opakuje, a které se

vyskytuje neustále nebo pravidelně. Pod pojem systematický spadá zpracování vyskytující se podle určitého systému, přednastavené nebo organizované, nebo vykonávané jako součást strategie.

Monitorování subjektu údajů není v Obecném nařízení rovněž definováno, v recitálu 24 je však vysvětlen pojem „monitorování chování subjektů údajů“, jenž zahrnuje sledování osob na internetu, včetně profilování těchto osob za účelem přijetí rozhodnutí ohledně subjektů údajů a analýzy jejich osobních preferencí, postojů a chování. Je však nutné podotknout, že monitorování osob se nemusí týkat pouze jejich online aktivit.

I v tomto případě platí, že pravidelné a systematické monitorování provádějí bezpečnostní agentury provozující kamerové systémy nebo provozovatelé sociálních sítí. Zcela jistě i finanční instituce a další povinné osoby dle AML zákona monitorují své klienty pravidelně a na základě určitého systému a následně vyhodnocují údaje o jejich rizikovosti.

Do třetí a poslední kategorie správců a zpracovatelů patří ty osoby, jejichž hlavní činnosti spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v čl. 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v čl. 10[105].

3.2.3 DOBROVOLNÉ JMENOVÁNÍ POVĚŘENCE

Obecné nařízení správcům a zpracovatelům nezakazuje, aby si svého pověřence jmenovali i v případě, kdy k tomu nejsou povinni. Zejména v případech, kdy si správci a zpracovatelé nebudou jisti, zda do některé z výše vymezených kategorií spadají, jsou

[105] čl. 10 Obecného nařízení:
„Zpracování osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření na základě čl. 6 odst. 1 se může provádět pouze pod dozorem orgánu veřejné moci nebo pokud je oprávněné podle práva Unie nebo členského státu poskytujícího vhodné záruky, pokud jde o práva a svobody subjektů údajů. Jakýkoli souhrnný rejstřík trestů může být veden pouze pod dozorem orgánu veřejné moci“.

oprávněni si pověřence jmenovat. Domnívám se však, že z důvodu nutnosti vynaložit na osobu pověřence další náklady, které budou už tak v důsledku implementace Obecného nařízení relativně vysoké, se k tomuto velká část správců a zpracovatelů neuchýlí do doby, než budou praxí jednotlivé podmínky zkonkretizovány.

V případě, kdy správce nebo zpracovatel pověřence jmenuje dobrovolně, je povinen plnit povinnosti stanovené v článcích 37 až 39 stejně jako osoby, které mají povinnost pověřence jmenovat. Zároveň však nic nebrání správcům, aby přijali zaměstnance a pověřili je některými úkoly souvisejícími s ochranou osobních údajů, aniž by byli v postavení pověřence a plnili všechny jeho povinnosti. V takovém případě je však správce nebo zpracovatel povinen jasně označit, že tato osoba není pověřencem.[106]

Již z právního vymezení jednotlivých osob, jež jsou pověřence povinni jmenovat, které není provedeno zcela určitě, je zřejmé, že v praxi některým správcům vznikne pochybnost, zda jsou pověřence skutečně povinni jmenovat. V těchto případech WP29 doporučuje, aby správce provedl důkladnou interní analýzu, v níž zohlední důležité faktory pro přijetí závěru, že pověřence je či není povinen jmenovat. Tato analýza by měla být průběžně aktualizována, zejména v případě, kdy správce nebo zpracovatel začne vykonávat nové činnosti nebo poskytovat nové služby, které by pod případy uvedené v čl. 37 odst. 1 mohly spadnout. Je rovněž nutné podotknout, že ÚOOÚ může správce a zpracovatele kdykoliv požádat, aby mu tuto analýzu poskytli.[107]

3.3 KVALIFIKACE POVĚŘENCE

Vzhledem k úloze, kterou pověřenec pro správce plní, je zřejmé, že k tomuto musí mít potřebné vědomosti a kvalifikaci. Konkrétně je dle čl. 37 odst. 5 Obecného nařízení nezbytné, aby měl potřebné profesní kvality spočívající zejména na odborných znalostech práva a praxe v oblasti ochrany údajů.

[106] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

[107] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

Z výše uvedeného ustanovení je zřejmé, že vymezení, zda je dána potřebná profesní kvalita pověřence, je nezbytné vnímat v několika rovinách. Zaprvé, je nutné, aby pověřenec měl dostatečnou úroveň odborných znalostí práva v oblasti ochrany údajů, která spočívá ve znalosti národní a evropské legislativy, zejména Obecného nařízení. Úroveň těchto odborných znalostí musí odpovídat povaze prováděného zpracování a rovněž citlivosti, složitosti a množství dat, které jsou správcem nebo zpracovatelem zpracovávány. Vedle odborných znalost je nutné, aby měl pověřenec dostatečnou znalost konkrétních procesů zpracování osobních údajů, které jsou správcem prováděny, včetně informací o jejich uložení a zabezpečení, a rovněž znalost oboru, v němž správce nebo zpracovatel podniká. Třetí rovinu profesní kvality pověřence tvoří schopnost pověřence plnit Nařízením stanovené úkoly. Pověřenec musí v rámci své organizace disponovat dostatečnými pravomocemi, aby veškeré úkoly mohl řádně vykonávat.[108]

Obecné nařízení nestanoví žádnou specifickou formu, kterou mohou být profesní kvality pověřence prokázány. Není tedy nezbytné, aby měl pověřenec například vysokoškolské vzdělání nebo absolvovanou některou profesní zkoušku. WP29 však ve svém stanovisku k pověřencům doporučuje, aby dozorové úřady propagovaly náležité a pravidelné školení pověřenců. Stále sice platí, že povinnost přijmout pouze proškoleného pověřence není Obecným nařízením stanovena, pokud však osoba ucházející se o funkci pověřence takové školení absolvovala, může to vypovídat o jejích dostatečných odborných znalostech práva osobních údajů.

Zároveň platí, že dozorové orgány jednotlivých členských států nejsou povinny školení pověřenců samy organizovat, úřadům je pouze doporučeno, aby školení pověřenců propagovaly. Český ÚOOÚ se k tomuto kroku zatím neuchýlil a žádné školení nepropaguje ani nepořádá. V České republice se však začíná vyskytovat několik různých soukromých subjektů, které za relativně vysoké ceny pořádají školení

[108] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

o ochraně osobních údajů pro pověřence, a po jejichž absolvování účastníci obdrží certifikát.[109]

Z výše uvedeného vymezení jednotlivých rovin, v nichž je nutné profesní kvalitu pověřence vnímat, však vyplývá, že by bylo velmi těžké určit univerzální kritéria, která mohou bezpečně určit osobu pro funkci pověřence nejvhodnější. Při vybírání osoby pověřence je vždy nutné zohlednit veškerá specifika daného správce, ať již jeho velikost, rozsah a složitost zpracování, které provádí, a včetně složitosti jeho poznání pro osobu mimo organizaci správce, nebo i skutečnost, zda je některý z jeho současných zaměstnanců vůbec schopen funkci pověřence vykonávat. Pouze s ohledem na všechny tyto skutečnosti pak může vhodného pověřence zvolit. V praxi tedy zpravidla nelze za dostatečnou kvalifikaci pověřence považovat jeho obecné proškolení z právních předpisů s ochranou osobních údajů souvisejících, je nezbytné zohlednit i jeho znalost konkrétních procesů zpracování správce, které se budou u valné většin správců lišit.

3.4 POSTAVENÍ POVĚŘENCE

V dalším ustanovení Obecného nařízení, které se pověřencům věnuje, tedy v čl. 38, nalezneme vymezení postavení pověřence v rámci organizace správce či zpracovatele i navenek.

Dle odst. 1 tohoto ustanovení je správce nebo zpracovatel povinen zajistit, aby byl pověřenec náležitě a včas zapojen do veškerých záležitostí souvisejících s ochranou osobních údajů. Požadavek včasnosti takového zapojení se projevuje například i v ustanovení č. 35 odst. 2 Obecného nařízení, kdy správci vzniká povinnost vyžádat si posudek pověřence při provádění posouzení vlivu na ochranu osobních údajů. Je tedy zřejmé, že pověřence je do jednotlivých procesů nezbytné zařadit již před samotným zpracováním osobních údajů.

[109] Např. http://www.tcox.cz/gdpr/kurz/poverenec-pro-ochranu-osobnich-udaju/ .

Z čl. 38 odst. 1 Obecného nařízení tedy vyplývá, že je správce povinen zajistit přítomnost pověřence u veškerých procesů zpracování osobních údajů a konzultovat je s ním, případně jej o nich řádně informovat. [110]

WP29 ve svém stanovisku k pověřencům doporučuje správci zakotvit následující konkrétní postupy pro zapojení pověřence:

- pověřenec by měl být pravidelně zván na schůze vyššího a středního managementu a rovněž na schůze, kde jsou přijímána rozhodnutí s dopadem do ochrany osobních údajů;
- pověřenec musí včas obdržet všechny podstatné informace o zpracování;
- stanovisku pověřence musí být vždy přiznána dostatečná váha a v případě, kdy se správce od takového stanoviska odchýlí, je povinen tento postup řádně odůvodnit a dokumentovat;
- pověřenec musí být bezodkladně informován a konzultován v případě porušení zabezpečení ochrany osobních údajů;
- je vhodné vypracovat směrnici nebo programy pro ochranu osobních údajů stanovující, kdy musí být pověřenec konzultován.

Odst. 2 stejného ustanovení správci a zpracovateli ukládá povinnost, aby podporovali pověřence při plnění jeho úkolů tím, že mu budou poskytovat zdroje nezbytné k plnění těchto úkolů, k přístupu k osobních údajům a operacím zpracování a k udržování jeho odborných znalostí. Podpora správce nebo zpracovatele by měla spočívat zejména v aktivní podpoře ze strany vyššího managementu, v poskytování dostatečné časové kapacity, ale i v poskytnutí dostatečné finanční a personální podpory.[111]

[110] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 342.

[111] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

Pověřenec dále dle Obecného nařízení nesmí dostávat žádné pokyny týkající se plnění jeho úkolů.[112] Nesmí být tedy správcem nebo zpracovatelem instruován, jakým způsobem má vykonávat svou funkci a rovněž mu nesmí být vnucován žádný právní názor.

Kromě plnění úkolů stanovených Obecným nařízením dále pověřenec slouží jako kontaktní místo pro subjekty údajů.[113] Ty se na něj mohou obracet ve všech záležitostech souvisejících se zpracováním jejich osobních údajů a výkonem jejich práv podle Obecného nařízení. To však neznamená, že pověřenec je jedinou osobou, na kterou se subjekty údajů mohou obrátit v případě, kdy chtějí uplatnit svá práva.

Vedle výše zmíněného je pověřenec dle čl. 38 odst. 5 vázán tajemstvím nebo důvěrností v souladu s právem Evropské unie nebo členského státu. Anglická verze Obecného nařízení v tomto ustanovení používá pojmy *„secrecy and confidentiality"*, které lze do češtiny volně přeložit i jako mlčenlivost. Ačkoliv český právní řád pojem mlčenlivost zná a používá, svou ustálenou legální definici nemá. V kontextu ustanovení čl. 38 odst. 5 Obecného nařízení však můžeme pod pojmem vázanosti mlčenlivostí (případně vázanosti tajemstvím nebo důvěrností) rozumět zejména zákaz jednání umožňujícího neoprávněným osobám seznámit se s informacemi, které pověřenec získal v souvislosti s výkonem své funkce.[114]

Návrh zákona o zpracování osobních údajů ustanovení čl. 38 Nařízení GDPR částečně upřesňuje a v § 12 stanoví, že pověřenec a fyzické osoby, které se podílejí na plnění jeho úkolů, jsou povinni zachovávat mlčenlivost o osobních údajích a bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů, se kterými se seznámili při plnění úkolů pověřence nebo v souvislosti s nimi. Tato povinnost trvá i po skončení výkonu činnosti pověřence nebo plnění jeho úkolů a nelze se jí dovolávat

---

[112] Čl. 38 odst. 3 Obecného nařízení.

[113] Čl. 38 odst. 4 Obecného nařízení.

[114] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 347.

vůči nelze dovolávat vůči správci nebo zpracovateli, který pověřence jmenoval, orgánu činnému v trestním řízení, soudu nebo úřadu a ohledně osobních údajů ani vůči subjektu údajů.

Ačkoliv je pověřenec dle Obecného nařízení oprávněn plnit i jiné úkoly a povinnosti než ty, které souvisí s výkonem funkce pověřence, je správce nebo zpracovatel povinen zajistit, aby žádné z těchto úkolů a povinností nevedly ke střetu zájmů.[115] Tento požadavek je v Obecném nařízení stanoven zejména z důvodu, aby nebyla ohrožena nezávislost funkce pověřence.

Ve střetu zájmů by se pověřenec ocitl zejména na takové pracovní pozici, na níž by měl pravomoc určovat účely a prostředky zpracování osobních údajů. Takové pravomoci mají zpravidla osoby ve vyšším managementu (např. výkonný ředitel, provozní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení), ke střetu zájmů však může dojít i u externího pověřence.[116] WP29 doporučuje, aby správce nebo zpracovatel předcházel vzniku střetu zájmů, a to například tím, že určí pracovní místa neslučitelná s výkonem funkce pověřence, sestaví vnitřní pravidla k zamezení střetu zájmů, a v případě uvolnění funkce pověřence a hledání pověřence nového dostatečně přesně a podrobně specifikovat, co může střet zájmů založit.

3.5 ÚKOLY POVĚŘENCE

Poslední článek Obecného nařízení, který se týká pověřence, je čl. 39, jež vyjmenovává úkoly, které pověřenec vykonává. Výčet, který je v tomto ustanovení podán, však není taxativní, jedná se pouze o minimální rozsah činností, které musí pověřenec vykonávat. Správce nebo zpracovatel jsou tedy oprávněni přidělovat pověřenci i další úkoly s ochranou osobních údajů související. Při stanovování takových dalších úkolů však správce a zpracovatel měl vždy zhodnotit, zda bude pověřenec schopen řádně vykonávat úkoly vymezené Obecným nařízením a že v takovém případě nevznikne střet zájmů.

---

[115] Čl. 38 odst. 6 Obecného nařízení.

[116] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

Obecné nařízení v čl. 39 odst. 1 stanoví pověřenci následující úkoly:

a) poskytování informací a poradenství správcům nebo zpracovatelům a jejich zaměstnancům;
b) monitorování souladu s Obecným nařízením;
c) poskytování poradenství při posuzování vlivu na ochranu osobních údajů;
d) spolupráce s dozorovým úřadem; a
e) působení jako kontaktní místo pro dozorový úřad.

Jak již bylo výše zmíněno, pověřenec musí vykazovat dostatečné profesní kvality, které spočívají i v odborných znalostech práva osobních údajů a Obecného nařízení. Tyto své znalosti musí být dle písm. a) pověřenec schopen předávat dál a umět Obecné nařízení vyložit všem zaměstnancům správce či zpracovatele. Pověřenec sice není povinen zajistit, aby všichni zaměstnanci správce či zpracovatele měli dokonalou znalost práva ochrany osobních údajů, měl by však činit takové kroky, aby byli tito zaměstnanci seznámeni se svými povinnostmi z Obecného nařízení vyplývajícími. Za tímto účelem by tedy měl vytvořit určitý informační kanál, který může spočívat zejména v organizaci školení nebo tvorbě informačních brožur.[117]

Dalším úkolem pověřence je monitorování souladu s Obecným nařízením. K jeho naplnění může pověřenec zejména shromažďovat informace o činnosti správce či zpracovatele a posuzovat, zda je takové zpracování v souladu s právními předpisy. Správci může následně dávat doporučení pro zajištění takového souladu.[118]

V případě kdy správce připravuje posouzení vlivů na ochranu osobních údajů dle čl. 35 Obecného nařízení, je povinen vyžádat si k tomuto posouzení od pověřence stanovisko, je-li jmenován. Samotné posouzení vlivu sice provádí správce a nikoliv

[117] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 349.

[118] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

pověřenec, ten by však pro správce měl posoudit několik otázek s posouzením vlivu souvisejících. Dle WP29 by se mělo jednat zejména o následující záležitosti:

- zda je nebo není nutné provést posouzení vlivu;
- jakou metodiku při zpracování posouzení vlivu použít;
- zda posouzení vlivu vypracovat vlastními silami nebo jeho zpracování zadat externě;
- jaká ochranná opatření (včetně technických a organizačních) uplatnit pro zmírnění rizik vůči právům a zájmům subjektů údajů;
- zda posouzení vlivu bylo zpracováno správce a zda jeho závěry (ať už vedou či ne k pokračován zpracovatelské operace a bez ohledu na to, jak ochranná opatření určují uplatnit) jsou v souladu s Obecným nařízením.[119]

Pověřenec je dále povinen spolupracovat s dozorovým úřadem a pro dozorový úřad působit jako kontaktní místo. Dozorovému úřadu tak má usnadnit plnění jeho úkolů a vyšetřovacích, nápravných, povolovacích a poradních pravomocí dle Obecného nařízení. Pověřenec může rovněž s dozorovým úřadem vést konzultace a žádat jej o rady v jakékoli věci související s ochranou osobních údajů.

3.6 USTANOVENÍ POVĚŘENCE

Další problematickou otázkou, kterou správci a zpracovatelé budou v souvislosti s aplikací Obecného nařízení řešit, je určení, v jakém právním postavení vůči nim pověřenec stojí. Vodítka k jejímu řešení podává samo Obecné nařízení, jež v čl. 37 odst. 6 stanoví, že pověřenec může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb.

Při jmenování pověřence musí správce a zpracovatel pamatovat zejména na veškeré požadavky, které na něj Obecné nařízení klade, a které spočívají jak v nezbytné úrovni jeho odborných znalostí a jiných schopností, tak v absenci střetu zájmů a postavení pověřence v organizaci, včetně přístupu k jejímu nejvyššímu vedení. Není

[119] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

vyloučeno, že osobu, která takové předpoklady splňuje, již správce nebo zpracovatel zaměstnává. V takovém případě mu Obecné nařízení nepřikazuje přijímat nového pracovníka a správce tak může využít některého ze současných zaměstnanců.

3.6.1 EXTERNÍ A INTERNÍ POVĚŘENEC

Z možností, které Obecné nařízení správci a zpracovateli pro přijetí pověřence dává, vyplývá, že existují v zásadě dva typy pověřenců, a to pověřenci interní, tedy osoby, které jsou pracovníky správce či zpracovatele, ať již nově najatí nebo u správce již dříve zaměstnaní, a externí, tedy osoby, s nimiž správce uzavírá smlouvu o poskytování služeb. Obecné nařízení nestanoví konkrétní případy, v nichž je nutné jmenovat pověřence interního nebo externího, volba mezi nimi tak leží zcela na správci a zpracovateli. Ten může sám uvážit, která z těchto možností je pro něj vhodnější či výhodnější.

Ke jmenování interního pověřence, zejména pak z řad současných zaměstnanců správce, v praxi zřejmě přikročí zejména větší organizace, které provádějí rozsáhlé a složité zpracování. Pro správce a zpracovatele tak bude výhodnější jmenovat do pozice pověřence osobu, která už je s procesy zpracování osobních údajů a s chodem organizace seznámena. V případě, kdy správce nebo zpracovatel provádí rozsáhlé zpracování, bude zřejmě docházet k situaci, kdy pověřenec bude natolik vytížen plněním svých úkolů, že nebude moci vykonávat žádné další činnosti. I z tohoto důvodu je tedy vhodné, aby byl v těchto případech zaměstnancem správce či zpracovatele a mohlo tak být zajištěno, že mu jiné úkoly nebudou přidělovány. Při jmenování interního pověřence však musí správce a zpracovatel pamatovat na to, aby jím nejmenoval osobu, která by mohla být ve střetu zájmů.[120]

V případě pověřence interního tedy bude mezi ním a správcem uzavřena pracovní smlouva a tento vztah se tedy bude řídit zákoníkem práce[121]. Z dikce Obecného

[120] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 340.

[121] V případě, kdy je správcem územní samosprávný celek, bude se jeho právní vztah s interním pověřencem řídit zákonem č. 312/2002 Sb., o úřednících územních samosprávných

nařízení vyplývá, že funkce pověřence má stálou povahu. Ministerstvo vnitra ve svém metodickém doporučení pro obce k zabezpečování funkce pověřence dovozuje, že pověřenec by z tohoto důvodu měl být u správce zaměstnán na základě pracovní smlouvy na dobu neurčitou. Ze stejného důvodu považuje Ministerstvo vnitra rovněž za nezbytné, aby funkce pověřence nebyla vykonávána na základě dohody o práci konané mimo pracovní poměr, vzhledem ke skutečnosti, že na takové dohody se dle ustanovení § 77 odst. 2 písm. g) ZPr neuplatní pravidla o skončení pracovního poměru. Zároveň však dle názoru Ministerstva vnitra není vyloučeno, aby v pracovní smlouvě byla sjednána zkušební doba. Ačkoliv zmíněná opatření jistě napomohou tomu, aby byla zajištěna nezávislost pověřence a oslabena možnost správce nebo zpracovatele jej z funkce odvolat bez nutnosti uvedení skutečných důvodů, takové jednání není založeno na požadavcích Obecného nařízení. To pouze stanoví, že pověřenec může být pracovníkem správce či zpracovatele, a nestanoví již další podmínky týkající se typu smlouvy, kterou s pracovníkem správce nebo zpracovatel uzavírá,[122] nebo jejích dalších náležitostí.[123]

Je nezbytné poznamenat, že mimo jiné se ZPr budou řídit i otázky týkající se odměňování interního pověřence.[124]

---

celků, neboť vykonává tzv. správní činnost dle tohoto zákona. Dle tohoto zákona se na úředníky územních samosprávných celků vztahuje zákoník práce, pokud tento zákon nestanoví jinak. Dále pak v případě, kdy je správcem ministerstvo nebo jiný správní úřad, jestliže je zřízen zákonem a je zákonem výslovně označen jako správní úřad nebo orgán státní správy, bude se jeho právní poměr s pověřencem řídit zákonem č. 234/2014 Sb., o státní službě.

[122] Tj. zda je skutečně nutné uzavřít pracovní smlouvu, nebo postačí uzavření dohody o pracích konaných mimo pracovní poměr.

[123] Tedy např. zakotvení zkušební doby nebo uzavření smlouvy na neurčito.

[124] Ministerstvo vnitra České republiky, 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.

Jak již bylo zmíněno, vedle interního pověřence mohou povinné subjekty jmenovat i pověřence externího. Ke jmenování externího pověřence bude zřejmě docházet zejména u menších a středních organizací, případně u orgánů veřejné moci či jiných veřejných subjektů, tedy zpravidla u subjektů, které neprovádí příliš rozsáhlé zpracování a nejsou tak schopny pověřence plně vytížit, a zároveň často nemají pro zřízení samostatné pozice potřebné peněžní prostředky.[125] Nevýhodou oproti interním pověřencům však je skutečnost, že externí pověřenci nemají tak dobrou znalost interních procesů v organizaci správce nebo zpracovatele.

Obecné nařízení výslovně stanoví, že funkci pověřence může vykonávat osoba, která není pracovníkem správce nebo zpracovatele, na základě smlouvy o poskytování služeb. Jedná se o soukromoprávní smlouvu, která by měla obsahovat následující náležitosti:

- označení osoby, která bude funkci pověřence vykonávat, a v případě, že se jedná o osobu právnickou rovněž označení jedné určité hlavní kontaktní osoby pro subjekty údajů a dozorový úřad;
- označení úkolů, které má pověřenec plnit;
- ujednání představující záruky nezávislosti výkonu funkce pověřence, zahrnující povinnost pověřence oznámit správci možný střet zájmů;
- závazek pověřence, že u něj nedojde ke střetu zájmů;
- závazek pověřence zachovávat mlčenlivost.[126]

I v případě výkonu funkce pověřence na základě smlouvy o poskytování služeb je nutné pamatovat, že má povahu stálou, a měla by tak být uzavírána na dobu neurčitou a ve smlouvě by měla být dohodnuta i výše odměny pověřence.

---

[125] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 341.

[126] Ministerstvo vnitra České republiky, 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.

Čl. 38 odst. 3 Obecného nařízení stanoví, že pověřenec nesmí být v souvislosti s plněním svých úkolů propuštěn ani sankcionován. Toto ustanovení napomáhá tomu, aby byla zajištěna nezávislost pověřenců a dostatečná ochrana při plnění svých úkolů.

Pověřence tedy není možné žádným způsobem postihovat, ani v oblasti odměňování či poskytování jiných výhod, které ostatní zaměstnanci správce požívají. Není nutné, aby tyto sankce byly dokonány, za dostačující se považuje i jejich hrozba.[127] Nelze jej postihovat za jakékoliv plnění svých povinností, a ani za skutečnost, že zastává jiný názor než správce. Není však vyloučeno, aby byl pověřenec propuštěn či sankcionován z důvodů, které nesouvisí s výkonem jeho úkolů, a to způsobem, který je v souladu se ZPr.

U externích pověřenců je vhodné zajistit splnění tohoto ustanovení tak, že ve smlouvě o poskytování služeb s nimi uzavřené bude zakotven taxativní výčet důvodů, pro něž může být tato smlouva vypovězena, a které nemohou záležet ve způsobu plnění úkolů pověřence.

Zákazem pověřence propustit či sankcionovat v souvislosti s plněním svých úkolů však není dotčena odpovědnost pověřence za škodu, kterou způsobí. To je dáno samotnou povahou institutu náhrady škody, jež je kompenzační a nikoliv sankční. Stejně tak se na interního pověřence vztahuje obecná úprava pracovního práva a není tedy vyloučeno, aby byl pověřenec propuštěn či sankcionován z jiných důvodů stanovených ZPr.[128] Není však zcela jisté, jakým způsobem budou řešeny případy, kdy pověřenec svým jednáním naplní některý z výpovědních důvodů stanovených ZPr, avšak stane se tak v souvislosti s plněním jeho úkolů. V praxi se bude jednat zejména o výpovědní důvody podle ustanovení § 52 písm. f) a g) ZPr, tedy nesplňuje-li zaměstnanec předpoklady pro výkon sjednané práce nebo z důvodu porušování

[127] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

[128] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 345.

povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci a z důvodů pro okamžité zrušení pracovního poměru. V případě, že by ustanovení čl. 38 odst. 3 Obecného nařízení bylo vykládáno extenzivně, zúžilo by to pravomoci správce vůči svým zaměstnancům stanovené ZPr. V důsledku uvedeného výkladu by však správce vůči pověřenci neměl žádný účinný prostředek ochrany v případě, že by pověřenec svou funkci nevykonával řádně.

Přikláním se proto k názoru, že by správce jako zaměstnavatel měl mít možnost pověřence postihnout tak, jak by v obdobných případech postihnul jiné své zaměstnance. Cílem ustanovení čl. 38 odst. 3 Obecného nařízení je ochrana pověřence a nezávislosti jeho funkce, nikoliv však jeho absolutní nedotknutelnost i v případě, kdy řádně neplní své úkoly.

Obecné nařízení nevylučuje, aby se pověřencem stala osoba právnická. Správci a zpracovatelé tak mohou jako pověřence jmenovat např. advokátní kancelář. I v těchto případech je však nezbytné, aby byla v rámci této právnické osoby určena konkrétní fyzická osoba, která bude dosažitelná pro dozorový úřad i pro správce, zpracovatele a jejich zaměstnance.[129] Z povahy věci vyplývá, že tento postup je možný pouze u pověřenců externích, a to z důvodu, že zaměstnancem může být dle ustanovení § 7 ZPr pouze fyzická osoba.

Lze předpokládat, že v roce 2018 a v následujících nejbližších letech přikročí ke jmenování externího pověřence i ti správci a zpracovatelé, pro něž by bylo v běžné situaci vhodnější jmenovat pověřence interního. Je totiž pravděpodobné, že v počátcích účinnosti Obecného nařízení bude velký nedostatek kvalifikovaných osob, které by funkci pověřence mohly vykonávat.

[129] Ministerstvo vnitra České republiky, 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.

Je nezbytné upozornit na skutečnost, že Obecné nařízení vznik funkce pověřence spojuje s pojmem „jmenování“. Vyvstává tedy otázka, zda takové pojmosloví implikuje, že se jedná o funkci založenou jmenováním dle § 33 odst. 3 ZPr. Zmíněné ustanovení sice stanovuje, že se pracovní poměr vedoucích zaměstnanců zakládá jmenováním v případech stanovených zvláštním právním předpisem, za který lze považovat i Obecné nařízení. V takovém případě by se však uplatnilo i ustanovení § 73 odst. 1 ZPr, jež stanoví, že ten, kdo je příslušný ke jmenování, může jmenovaného zaměstnance z pracovního místa odvolat, a to i bez udání důvodu. Takového oprávnění by správce jako zaměstnavatel mohl snadno zneužívat a obcházet tak povinnost stanovenou čl. 38 odst. 3 Obecného nařízení, tedy že pověřenec nesmí být v souvislosti s plněním svých úkolů propuštěn ani sankcionován. Rovněž je nutné podotknout, že jmenováním se zakládá pracovní poměr pouze u vedoucích zaměstnanců, přičemž v pozici vedoucího zaměstnance by pověřenec z důvodu střetu zájmů neměl být. Z těchto důvodů se domnívám, že byl při provádění českého překladu Obecného nařízení v tomto případě zvolen ne zcela přesný pojem „jmenování“, jenž nelze ztotožňovat se jmenováním dle ZPr.

3.6.2 SDÍLENÍ POVĚŘENCE

Čl. 37 odst. 2 Obecného nařízení dovoluje skupině podniků jmenovat jediného společného pověřence, odst. 3 stejného ustanovení to pak umožňuje i několika orgánům veřejné moci nebo veřejným subjektům.

Dle odst. 2 tohoto ustanovení je nezbytné, aby byl pověřenec jmenovaný pro skupinu podniků pro každý z těchto subjektů snadno dostupný. Dostupnost pověřence spočívá jednak v podmínce, aby byly všem subjektům údajů a zaměstnancům správce zpřístupněny jeho kontaktní údaje, jednak v jeho dosažitelnosti. Dosažitelnost nutně nemusí spočívat ve fyzické přítomnosti pověřence na pracovišti správce, pro jeho kontaktování je možné využívat prostředky komunikace na dálku. Jinými slovy, subjekty údajů a zaměstnanci správce či zpracovatele musí být schopny pověřence snadno kontaktovat. Při jmenování pověřence pro několik orgánů veřejné moci nebo veřejných subjektů dle odst. 3 stejného ustanovení je nezbytné, aby byl jmenován s přihlédnutím k jejich organizační struktuře a velikosti.

Z výše uvedeného vyplývá, že je správce vždy povinen zajistit, aby byl pověřenec schopen řádně plnit veškeré své úkoly i v případě, kdy je jmenován pro několik subjektů. Pověřenec však veškeré úkoly Obecným nařízením stanovené nemusí vykonávat sám, k dispozici může mít několik dalších pracovníků, které mu s plněním povinností budou napomáhat a pověřenec tak může spolupracovat s větším množstvím správců a zpracovatelů.

Obecné nařízení konkrétně nestanoví, pro jaký maximální počet subjektů může být stanoven jeden společný pověřenec a tento počet je nutné určit vždy s ohledem na specifika konkrétních správců nebo zpracovatelů. Určité vodítko k určení tohoto počtu podává Ministerstvo vnitra České republiky ve svém metodickém doporučení k činnosti obcí k zabezpečení funkce pověřence, které doporučuje, aby byl jeden pověřenec stanoven nejvýše pro 10 obcí. Je však nutné poznamenat, že toto doporučení se vztahuje na případy, kdy pověřence vykonává pouze jedna fyzická osoba bez jakéhokoliv spolupracujícího týmu. Zároveň je vždy nezbytné zohlednit specifika konkrétního správce či zpracovatele, včetně jeho velikosti a rozsáhlosti a složitosti jeho procesů zpracování osobních údajů. Metodický pokyn Ministerstva vnitra České republiky lze vnímat pouze jako doporučující dokument a nikoliv jako závazný právní předpis; pokud tedy správce nebo zpracovatel ve své analýze dospěje k závěru, že pověřence využije pouze v malém rozsahu, nelze vyloučit, že jeden pověřenec bude schopen svou funkci vykonávat i pro více než 10 obcí.

Společného pověřence může vykonávat jak pověřenec interní, tak externí. Je však nutné pamatovat, že v případě, kdy je správcem nebo zpracovatelem územní samosprávný celek, který jmenuje pověřence interního, tedy pověřence, který má s každým správcem či zpracovatelem uzavřenou pracovní smlouvu, vztahuje se na pověřence omezení dané ustanovením § 16 odst. 4 zákona č. 312/2002 Sb., o úřednících územních samosprávných celků, podle něhož může úředník vykonávat jinou výdělečnou činnost jen s předchozím písemným souhlasem územního samosprávného celku, u něhož je zaměstnán. Obdobná omezení je zakotveno i v zákonu č. 234/2014 Sb., o státní službě, dle jehož ustanovení § 81 odst. 2 může státní zaměstnanec vykonávat jinou výdělečnou činnost než službu podle tohoto zákona

pouze s předchozím písemným souhlasem služebního orgánu. Není samozřejmě vyloučeno, že pověřenec externí má ve své smlouvě o poskytování služeb sjednanou doložku s obdobným obsahem, i na tuto skutečnost tedy správce musí pamatovat.[130]

Obecným nařízením dále nejsou vymezeny případy, kdy by společný pověřenec musel být jmenován, vždy tak bude záležet na dobrovolném rozhodnutí správce či zpracovatele.

WP29 považuje za vhodné, aby pověřenec sídlil v Evropské unii, a to bez ohledu na skutečnost, zda je správce nebo zpracovatel v Evropské unii usazen.[131]

[130] Ministerstvo vnitra České republiky, 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.
[131] WP29 Guidelines on Data Protection Officers (‘DPOs’) (*překlad vlastní*).

IV. ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

4.1 ZABEZPEČENÍ ZPRACOVÁNÍ

Povinnost zajištění řádného zabezpečení osobních údajů spadá mezi základní povinnosti správce při zpracování osobních údajů, a je zařazena mezi základní zásady zpracování osobních údajů v čl. 5 Obecného nařízení. Další povinnosti se zabezpečením osobních údajů související jsou blíže upraveny v Kapitole IV., Oddílu 2 Obecného nařízení.

Ačkoliv s účinností Obecného nařízení přibydou správci a zpracovateli některé zcela nové povinnosti, zabezpečení osobních údajů je správce a zpracovatel povinen zajistit již dle současného OchOsÚ. Správce či zpracovatel je dle § 13 OchOsÚ povinen posoudit rizika, která při zpracování osobním údajům hrozí, a následně přijmout technicko-organizační opatření, aby nemohlo dojít k neoprávněnému přístupu k nim nebo k jejich jinému zneužití. Obecné nařízení nově upřesňuje, že je správce či zpracovatel při posouzení rizik pro osobní údaje povinen přihlédnout ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování.[132]

Správce nebo zpracovatel by měl dle Obecného nařízení při zjišťování vhodné úrovně zabezpečení zohlednit riziko, zda dojde k náhodnému nebo protiprávnímu zničení, ztrátě, pozměňování, či neoprávněnému zpřístupnění osobních údajů. Posuzování, zda k některému riziku může dojít, by správce a zpracovatel neměli provádět pouze jednorázově, nýbrž pravidelně v průběhu zpracování. Zároveň by neměli zohledňovat pouze rizika, která představují softwarové systémy, ale i lidský faktor a fyzické prostředí, v němž jsou softwarové systémy nebo přímo samotné osobní údaje umístěny.[133]

---

[132] Čl. 32 odst. 1 Obecného nařízení.

[133] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 292.

Obecné nařízení v čl. 32 odst. 1 podává následující výčet opatření, které může správce či zpracovatel přijmout, aby zajistil úroveň zabezpečení odpovídající riziku:

a) pseudonymizace a šifrování osobních údajů;
b) opatření pro zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování;
c) opatření pro zajištění schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
d) zavedení procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Tento výčet je však pouze příkladmý, správce není povinen všechna tato opatření přijmout, a zároveň ani není stanoveno, že přijetí všech vyjmenovaných opatření bude pro zabezpečení dostačující. Platí tedy, že správce či zpracovatel je vždy povinen zohlednit specifika konkrétního zpracování.

Jak již bylo výše blíže vysvětleno, pseudonymizace je proces, při němž jsou odděleny přímé identifikátory subjektů údajů od jiných, nepřímých identifikátorů. Přímé identifikátory jsou pak uchovávány odděleně od identifikátorů nepřímých. V případě, kdy neoprávněná osoba získá k pseudonymizovaným údajům přístup, nebude je schopna přiřadit ke konkrétnímu subjektu údajů, aniž by současně získala přístup i k dodatečným informacím, které subjekt údajů přímo identifikují. Šifrování je pak procesem, jenž převede osobní údaje do podoby, která není čitelná bez znalosti zvláštní informace, tj. šifrovacího klíče.[134]

Správce či zpracovatel by dále měl zavést opatření pro zajištění neustálé důvěrnosti, integrity, dostupnosti a odolnosti systémů a služeb zpracování. Takové opatření se skládá z několika jednotlivých dílčích bezpečnostních opatření.

---

[134] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 293.

První takovou skupinou jsou opatření pro zajištění důvěrnosti systémů a služeb zpracování, které může spočívat jednak ve výše zmíněné pseudonymizaci a šifrování, jednak ve využití systémů autentizace a autorizace, které zajistí umožnění přístupu do systémů pouze oprávněným osobám. Dalším aspektem je zajištění integrity systémů a služeb zpracování. To spočívá v ochraně osobních údajů před neoprávněným zničením, ztrátou či pozměněním, tedy v zajištění konzistentnosti, přesnosti a důvěryhodnosti systémů a služeb zpracování. Správce či zpracovatel by tak měl zavést opatření, která jsou schopna monitorovat zejména údaje o přístupu konkrétních osob k osobním údajům a změn, které tyto osoby provedly. Systémy a služby zpracování by dále měly být neustále dostupné. Správce či zpracovatel by tak měli zajistit záložní zdroje, které budou k dispozici v případě výpadku či poškození hlavního systému. S požadavkem dostupnosti úzce souvisí další skupina bezpečnostních opatření, která spočívají v odolnosti systémů. Systémy a služby zpracování by měly být schopny odolávat různým selháním a v případě, že takové selhání nastane, mely by zachovávat bezpečnost osobních údajů.[135]

Další bezpečnostní opatření, které by měl správce zajistit, je schopnost obnovit dostupnost osobních údajů a přístup k nic včas v případě fyzických či technických problémů. V případě, kdy dojde ke znemožnění přístupu k osobním údajům, měla by správci zavedená bezpečnostní a technická opatření umožnit co nejrychlejší obnovu tohoto přístupu.

Podle písm. d) ustanovení čl. 32 odst. 1 Obecného nařízení je správce a zpracovatel povinen provádět pravidelné posuzování účinnosti zavedených opatření. Správce či zpracovatel by tak měl průběžně hodnotit a testovat jednak samotná bezpečnostní opatření, jednak míru rizika zpracování. V případě, kdy během zpracování dojde ke změně míry rizika, které zpracování představuje, měl by tomu být správce či zpracovatel schopen bezpečnostní opatření přizpůsobit.

---

[135] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 294.

Kromě technicko-organizačních opatření, která jsou zmíněna v čl. 32 odst. 1 Obecného nařízení, je správce dle odst. 4 stejného ustanovení povinen přijmout opatření pro zajištění toho, aby fyzické osoby, které mají k osobním údajům přístup, zpracovávaly tyto osobní údaje pouze na pokyn správce. Tato povinnost se však nevztahuje na případy, kdy je zpracování uloženo právem Evropské unie nebo členského státu. Správce by tedy měl svým zaměstnancům, kteří s osobními údaji pracují, podat jednoznačné pokyny, jakým způsobem s osobními údaji nakládat, a to v rámci pracovní smlouvy nebo vnitřního předpisu.[136]

4.2 OHLAŠOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ DOZOROVÉMU ÚRADU

4.2.1 DEFINICE PORUŠENÍ ZABEZPEČENÍ

Povinností, kterou Obecné nařízení v čl. 33 nově zavádí pro všechny správce, je povinnost ohlašování případů porušení zabezpečení osobních údajů (dále jen „porušení zabezpečení“) dozorovému úřadu. Český právní řád již však obdobnou povinnost zná i v současné době, týká se však pouze povinných osob dle zákona č. 127/3005 Sb., o elektronických komunikacích nebo dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Porušení zabezpečení osobních údajů je Obecným nařízením definováno jako porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů. K takovému porušení může dojít jak zvenčí organizace správce, tak zevnitř, a to jak úmyslně, tak nedbalostně.[137]

---

[136] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 295.

[137] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 93.

Z výše uvedeného je zřejmé, že porušení zabezpečení může dojít několika různými způsoby. Na základě toho WP29 ve svém stanovisku k ohlašování případů porušení zabezpečení[138] rozlišuje celkem tři druhy porušení zabezpečení, a to porušení důvěrnosti (*confidentiality breach*), které zahrnuje případy, kdy dojde k neoprávněnému zveřejnění či zpřístupnění osobních údajů, dále pak porušení dostupnosti (*availability breach*), tj. ztráta přístupu k osobním údajům, případně jejich zničení nebo ztráta, a porušení integrity (*integrity breach*), tj. případy neoprávněného pozměnění osobních údajů.

Všechny případy porušení zabezpečení však není nutné dozorovému úřadu oznamovat. Obecné nařízení v čl. 33 odst. 1 stanovuje výjimku pro takové porušení, u něhož je nepravděpodobné, že by mělo za následek riziko pro práva a svobody fyzických osob. Takovým případem může být zejména porušení zabezpečení osobních údajů, které jsou již veřejně dostupné.[139] Správce by tak měl vždy posoudit, jaké riziko dané porušení zabezpečení představuje, a jaké dopady může mít na práva a svobody fyzických osob, a teprve na základě tohoto posouzení se rozhodnout, zda se na danou situaci výjimka skutečně vztahuje.

Je nutné podotknout, že Obecné nařízení stanoví, že správce je povinen posoudit riziko porušení zabezpečení pro práva a svobody jakýchkoliv fyzických osob. Výjimka z oznamovací povinnosti správce se tak uplatní pouze v případě, kdy správce dospěje k závěru, že není pravděpodobný vznik rizika pro práva a svobody jakýchkoliv fyzických osob, a nikoliv pouze subjektů údajů.

Pokud dojde k případům, kdy správce ztratí přístup k osobním údajům pouze dočasně, případně k jinému porušení zabezpečení, které nebude mít výrazné dopady do sféry subjektu údajů, není správce povinen provést oznámení porušení zabezpečení. Výše

---

[138] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

[139] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

zmíněné však správce nezbavuje povinnosti zdokumentovat veškeré porušení zabezpečení, včetně takových porušení, která neměla vliv na práva a svobody fyzických osob[140].

Újma, která může subjektu údajů v důsledku porušení zabezpečení vzniknout, může být různého charakteru. Obecné nařízení v recitálu 85 uvádí jako možné následky fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad osobními údaji nebo omezení práv fyzických osob diskriminace, krádež nebo zneužití identity, finanční ztráta, neoprávněné zrušení pseudonymizace, poškození pověsti, ztráta důvěrnosti osobních údajů chráněných služebním tajemstvím nebo jakékoliv jiné významné hospodářské či společenské znevýhodnění dotčených fyzických osob.

Je nutné poznamenat, že oznamovací povinnost se vztahuje pouze na správce osobních údajů, tedy nikoliv na zpracovatele. Zpracovatel je však dle čl. 33 odst. 2 povinen bez zbytečného odkladu správci oznámit jakékoliv porušení zabezpečení osobních údajů. Zpracovatel tak podobně jako správce bude povinen provést posouzení, zda k porušení zabezpečení skutečně došlo.

4.2.2 OKAMŽIK PORUŠENÍ ZABEZPEČENÍ

Dle čl. 32 odst. 1 Obecného nařízení je správce povinen porušení zabezpečení ohlásit dozorovému úřadu do 72 hodin od okamžiku, kdy se o něm dozvěděl. Určujícím momentem pro počátek běhu této lhůty je tedy okamžik, kdy se správce o porušení zabezpečení dozvěděl.

Dle WP29 lze za okamžik, kdy se správce o porušení zabezpečení dozvěděl, považovat chvíli, kdy měl již správce přiměřenou míru jistoty, že došlo k porušení zabezpečení, které ohrozilo osobní údaje. Toto vodítko však není o mnoho přesnější než samotné znění Obecného nařízení a počátek běhu lhůty pro podání oznámení rovněž jednoznačně neurčuje. Lze však říci, že se správce o porušení zabezpečení dozvěděl ve chvíli, kdy z dostatečně věrohodného zdroje získal informaci o konkrétní

[140] Čl. 33 odst. 5 Obecného nařízení.

skutečnosti, která představuje porušení zabezpečení. Takovým věrohodným zdrojem může být zejména zaměstnanec správce, případně i osoba zvenčí organizace správce, která správci oznámí, že jí byly osobní údaje zpřístupněny. Jiným příkladem může být situace, kdy správce prokazatelně zjistí, že do jeho interního systému, v němž jsou osobní údaje uloženy, pronikla neoprávněná osoba.[141]

V případě, kdy správce nestihne oznámení porušení zabezpečení učinit do 72 hodin od okamžiku, kdy se o něm dozvěděl, musí současně s ním uvést důvody tohoto zpoždění.[142] Lze předpokládat, že dozorový úřad v takových případech nebude považovat za polehčující okolnost skutečnosti, že správce neměl přijata dostatečná opatření pro odhalování a oznamování porušení zabezpečení.[143]

Jak již bylo zmíněno, aby se na správce mohla vztahovat povinnost ohlásit porušení zabezpečení, musí se nejprve správce o takovém porušení dozvědět. Je však nutné poznamenat, že schopnost správce včas odhalit a ohlásit porušení zabezpečení je jedním ze základních znaků řádného přijetí bezpečnostních opatření dle čl. 32 Obecného nařízení.[144] Pokud se tedy správce o porušení zabezpečení včas nedozví, může to znamenat, že porušil některou ze svých dalších povinností dle Obecného nařízení, a to zejména povinnost integrity, důvěrnosti a řádného zabezpečení osobních údajů.

4.2.3 OBSAH OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ

Minimální nezbytné náležitosti ohlášení porušení zabezpečení vyjmenovává Obecné nařízení v čl. 33 odst. 3.

---

[141] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

[142] Čl. 33 odst. 1 Obecného nařízení.

[143] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 301.

[144] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

První z požadovaných náležitostí je popis povahy daného případu porušení zabezpečení včetně, pokud je to možné, kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů. Správce by tedy měl popsat, jakým způsobem a za jakých okolností k porušení zabezpečení došlo. Obecné nařízení samo nevymezuje, jakým způsobem má správce uvést kategorii subjektů údajů či osobních údajů. WP29 však uvádí[145], že pro kategorizaci subjektu údajů může být zejména relevantní, zda je dotčený subjekt údajů dítětem, osobou se zdravotním či tělesným postižením, zaměstnancem, či spotřebitelem. Při kategorizaci osobních údajů by měl správce zohlednit, jaký následek může neoprávněný přístup k těmto osobním údajům pro subjekt údajů představovat, zejména riziko krádeže identity, podvodu nebo vyzrazení obchodního tajemství.

Obecné nařízení předpokládá, že správce nebude vždy schopen uvést přesný počet subjektů údajů a osobních údajů porušením zabezpečení dotčených. V takových případech postačí uvedení pouze přibližného počtu.

V případě, že je u správce zřízena funkce pověřence osobních údajů, je povinen do ohlášení uvést jeho jméno a kontaktní údaje. V případě, že tomu tak není, měl by správce uvést jiné kontaktní místo, které bude s dozorovým úřadem komunikovat.

Dle čl. 33 odst. 3 písm. c) je správce dále povinen uvést popis pravděpodobných důsledků porušení zabezpečení osobních údajů. Měl by přitom zohlednit, jakou újmu může porušení zabezpečení představovat pro fyzické osoby.[146]

Jako poslední nezbytnou náležitost ohlášení porušení zabezpečení uvádí Obecné nařízení popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení zabezpečení osobních údajů, včetně případných opatření ke zmírnění

---

[145] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

[146] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 302.

možných nepříznivých dopadů. Na základě tohoto popisu pak dozorový úřad bude posuzovat, zda správce na porušení zabezpečení dostatečně zareagoval, nebo zda bude nutné vůči správci uplatnit některou z pravomocí dozorového úřadu.[147]

Výčet, který Obecné nařízení v čl. 33 odst. 1 podává, není taxativní, správce tak může v rámci ohlášení uvést i další informace, které považuje za vhodné.

V případě, že není možné výše zmíněné informace poskytnout současně, může je správce poskytnout postupně bez dalšího zbytečného odkladu.[148] To usnadňuje postup správci v případě, kdy nemá veškeré potřebné informace k podání ohlášení k dispozici v zákonné lhůtě. WP29 doporučuje, aby v těchto případech správce v průběhu informoval dozorový úřad, že mu část potřebných informací bude poskytnuta později.[149]

4.2.4 KOLIZE OHLÁŠENÍ PORUŠENÍ ZABEZPEČENÍ SE ZÁSADOU NEMO TENETUR

V případě, kdy správce řádně neprovede ohlášení porušení zabezpečení, může být takové jednání dozorovým úřadem právně kvalifikováno jako přestupek, přičemž za takové jednání může být dozorovým úřadem uložena pokuta až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2% celkového ročního obratu, podle toho, která hodnota je vyšší.[150]

Skutečnost, že ohlášení porušení zabezpečení nebylo včas a řádně provedeno, však může odhalit, že správcem nebyly splněny jiné povinnosti stanovené Obecným nařízením, zejména že nebyla zavedena dostatečná bezpečnostní opatření dle čl. 32. V takových případech není vyloučeno, že správce bude odpovědný za dva různé

---

[147] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 303.

[148] Čl. 33 odst. 4 Obecného nařízení.

[149] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

[150] Čl. 83 odst. 4 písm. a) Obecného nařízení.

přestupky, přičemž prvním z nich je nesplnění povinnosti ohlásit porušení zabezpečení a druhým z nich je nedostatečné zabezpečení osobních údajů.[151]

Obdobný postup platí i v případech, kdy správce řádně ohlásí porušení zabezpečení, a takové ohlášení odhalí, že správce porušil některou svou povinnost Obecného nařízení zejména dle čl. 32. I v takových případech může být správci uložena sankce za nesplnění takové povinnosti.

Vyvstává tedy otázka, jakým způsobem budou tyto situace ÚOOÚ posuzovány, a to s ohledem na ústavní pořádek České republiky.

Jednou ze základních ústavních zásad, které v České republice platí, je zásada nemo tenetur se ipsum accusare (*„nikdo není povinen sám sebe obviňovat“*, dále jen „**nemo tenetur**“). V ústavním pořádku je vyjádřena v čl. 37 odst. 1 LZPS, jenž stanoví, že každý má právo odepřít výpověď, jestliže by jí způsobil nebezpečí trestního stíhání sobě nebo osobě blízké a rovněž v čl. 40 odst. 4 LZPS, jenž zakotvuje právo obviněného odepřít výpověď. Rozsahem použití zásady nemo tenetur se již opakovaně zabýval i Ústavní soud České republiky.

Ústavním soudem bylo judikováno, že z ustanovení čl. 37 a 40 LZPS vyplývá i zákaz vydávání věcí a důkazů proti sobě samému. Obviněnému tak není možné ukládat pořádkové pokuty k vynucení předložení takových důkazů.[152] Lze si tedy položit

---

[151] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

[152] Nález Ústavního soudu České republiky ze dne 8. 11. 2005, sp. zn. I. ÚS 402/05:
„Povinnost k vydání věci ve smyslu § 78 trestního řádu zavazuje každého, avšak pokud jde o osobu, u které trestní řízení nepochybně směřuje k jejímu obvinění, případně jde přímo o osobu obviněnou, nelze vynucovat splnění této povinnosti ukládáním pokut podle § 66 odst. 1 trestního řádu. Jednalo by se totiž o donucování k poskytnutí důkazů proti sobě samému, jehož zákaz vyplývá z ustanovení čl. 37 odst. 1 a čl. 40 odst. 4 Listiny základních práv a svobod, čl. 14 odst. 3 písm. g) Mezinárodního paktu o občanských a politických právech a rovněž je, v souladu s judikaturou Evropského soudu pro lidská práva, obsažen v pojmu spravedlivého

otázku, zda lze předložení ohlášení porušení zabezpečení považovat za předložení důkazu proti sobě samému. Jistě tomu tak v některých případech může být.

V nálezu ze dne 11. 10. 2007, sp. zn. III. ÚS 528/06, však Ústavní soud poznamenal, že právo nemo tenetur nelze aplikovat zcela neomezeně. Ačkoliv obviněný zcela jistě nesmí být nucen k aktivnímu jednání, je povinen pasivně strpět úkony orgánů činných v trestních řízení. Podávání ohlášení porušení zabezpečení je však zcela jistě jednáním aktivním.

Ačkoliv se dle znění ustanovení čl. 37 a 40 LZPS zásada nemo tenetur uplatní pouze v případě trestního stíhání, Ústavní soud již v minulosti dovodil, že se vztahuje i na řízení správní, tedy i na přestupky.[153] Zde je však nutné poznamenat, že jednání správce může dosahovat i intenzity trestného činu, a to konkrétně trestného činu neoprávněného nakládání s osobními údaji dle ustanovení § 180 zákona č. 40/2009, trestního zákoníku.

V příštích letech bude tedy nepochybně zajímavé sledovat, jakým způsobem s kolizí povinnosti ohlašování porušení zabezpečení a zásady nemo tenetur naloží jak ÚOOÚ, tak zejména soudy České republiky.

řízení uvedeného v čl. 6 Úmluvy o ochraně lidských práv a základních svobod. K získávání důkazů orgány činnými v trestním řízení je v tomto případě možno využít zajišťovací úkon odnětí věci dle § 79 trestního řádu, který je pouze snášen, na rozdíl od ukládání pořádkových pokut, kterými se vyžaduje volní aktivní činnost, a proto přípustné není.“

[153] Nález Ústavního soudu České republiky ze dne 18. 2. 2010, sp. zn. I. ÚS 1849/08: *„Svobodný jednotlivec, jako součást občanské společnosti, nemůže být v právním státě partnerem správního orgánu vykonávajícího vrchnostenská oprávnění. Má naopak povinnost se takovým opatřením podrobit, jsou-li vykonávána řádně, tj. nejde-li o exces. Tak také nelze pokutovat osobu, která odmítne podat správnímu orgánu vysvětlení v případě, kdy je zřejmé, že by jím, byť i jen teoreticky, mohla přispět ke svému postihu za přestupek“*.

4.3 OZNAMOVÁNÍ PŘÍPADŮ PORUŠENÍ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ SUBJEKTU ÚDAJŮ

Vedle ohlašování případů porušení zabezpečení dozorovému úřadu je správce dle čl. 34 Obecného nařízení povinen ve stanovených případech oznámit porušení zabezpečení osobních údajů subjektu údajů.

Porušení zabezpečení je správce povinen subjektu údajů oznámit pouze pokud je pravděpodobné, že takové porušení bude mít za následek vysoké riziko pro práva a svobody fyzických osob.[154] Rozsah případů, kdy je oznámení subjektu údajů správce povinen učinit, je tedy užší než v případě ohlášení porušení zabezpečení dozorovému úřadu.

Obdobně jako v případě ohlašování porušení zabezpečení dozorovému úřadu by měl správce nejprve provést analýzu a posoudit, jaký dopad může mít dané porušení zabezpečení na práva a svobody fyzických osob. Zároveň by měl správce zohlednit, jaký újma těmto osobám může vzniknout. Pouze v případě, kdy správce dospěje k závěru, že riziko pro práva a svobody fyzických osob je vysoké, je povinen subjektu údajů porušení zabezpečení oznámit.

I v případě, kdy dle posouzení správce riziko pro práva a svobody osob vysoké není, může mu dozorový úřad nařídit, aby provedl oznámení porušení zabezpečení subjektu údajů. Dozorový úřad tak může učinit v případě, kdy v konkrétním případě sám provede posouzení rizika a dospěje k závěru, že vysoké riziko dáno je.[155]

V čl. 34 odst. 3 jsou stanoveny podmínky, kdy při splnění některé z nich správce není povinen oznamovat subjektu údajů porušení zabezpečení i v případě, kdy představuje vysoké riziko pro práva a svobody osob. První z nich je případ, kdy správce zavedl náležitá technická a organizační ochranná opatření, která byla použita u dotčených osobních údajů. To platí zejména v případě, kdy taková opatření zajišťují

[154] Čl. 34 odst. 1 Obecného nařízení.

[155] Čl. 34 odst. 4 Obecného nařízení.

nesrozumitelnost osobních údajů pro neoprávněné osoby. Pokud tedy byly osobní údaje zajištěny např. šifrováním, není správce povinen subjekt údajů informovat.

Stejné platí i v případě, kdy správce po porušení zabezpečení přijal opatření, která zajistí, že vysoké riziko pro práva a svobody subjektu údajů se již pravděpodobně neprojeví. Jedná se tedy o situaci, kdy již riziko pro práva a svobody fyzických osob vzniklo, správce však následně zajistil, aby nemělo žádný vliv na práva a svobody osob. Poslední možností, kdy správce nemusí subjektu údajů oznamovat porušení zabezpečení, je v případě, kdy by to vyžadovalo nepřiměřené úsilí. V takovém případě však musí být subjekty údajů informovány pomocí veřejného oznámení nebo podobného opatření.

Vedle toho, že je dozorový úřad dle čl. 34 odst. 4 oprávněn nařídit správci, aby subjektu údajů oznámil porušení zabezpečení, může rovněž rozhodnout, že je splněna některá z podmínek uvedených v odst. 3.

Čl. 34 na rozdíl od čl. 33 nestanoví správci maximální lhůtu 72 hodin, v níž musí oznámení porušení zabezpečení provést. I tak ale platí, že je povinen oznámení subjektu údajů učinit bez zbytečného odkladu.

Oznámení porušení zabezpečení subjektu údajů je správce povinen provést za použití jasných a jednoduchých jazykových prostředků. Je tedy nezbytné, aby bylo subjektu údajů oznámení vysvětleno srozumitelně a tak, aby jej jednoznačně pochopil. Oznámení porušení zabezpečení by tedy nemělo být součástí jiného sdělení, jako je např. newsletter nebo jiné pravidelné oznámení. Zároveň je v případech skutečně vysokého rizika vhodné, aby správce oznámení učinil prostřednictvím několika kontaktních prostředků.[156]

[156] WP29, Guidelines on Personal Data Breach Notification under Regulation 2016/679 (*překlad vlastní*).

Dle čl. 34 odst. 2 musí přinejmenším obsahovat informace uvedené v čl. 33 odst. 3 písm. b), c) a d), tedy jméno a kontaktní údaje pověřence nebo jiného kontaktního místa, popis pravděpodobných důsledků porušení zabezpečení a popis opatření, které správce přijal nebo navrhl k přijetí, aby dané porušení zabezpečení vyřešil.

4.4 POVINNOST ZAMĚSTNANCŮ SPRÁVCE OZNAMOVAT PORUŠENÍ ZABEZPEČENÍ

Jeví se vhodným rovněž uvést, že povinnost oznamovat porušení zabezpečení vyplývá z Obecného nařízení pouze správci, potažmo zpracovateli. Dle mého názoru by nebylo správné bez dalšího tuto povinnost na základě Obecného nařízení rozšiřovat i na zaměstnance správce způsobem, aby i tito zaměstnanci měli povinnost ohlašovat svému zaměstnavateli porušení zabezpečení. To ovšem nemusí vylučovat existenci fakticky obdobné povinnosti z jiných právních důvodů.

Zcela jistě platí, že zaměstnanec musí při výkonu práce dodržovat pokyny zaměstnavatele, stejně jako musí při práci dodržovat povinnosti vyplývající mu z právního řádu.[157] Zaměstnanec má rovněž povinnost pracovat řádně podle svých znalostí a schopností[158] a počínat si tak, aby nedocházelo k majetkové či nemajetkové újmě.[159]. Hrozí-li škoda nebo nemajetková újma, je povinen na ni upozornit nadřízeného vedoucího zaměstnance.[160] Zaměstnanec je také povinen zakročit, pokud je to nutné pro odvrácení nebezpečí vzniku škody zaměstnavateli.[161] Současně se uplatní zásada *ignorantia legis non excusat* a neznalostí právního řádu[162] proto nelze omluvit porušení zákonných povinností.

Na tomto místě je vhodné zmínit i čl. 32 odst. 4 Obecného nařízení, na jehož základě jsou správce a zpracovatel povinni přijmout opatření pro zajištění, aby každá fyzická

[157] § 301 písm. c) ZPr.

[158] § 301 písm. a) ZPr.

[159] § 249 odst. 1 ZPr.

[160] § 249 odst. 1 ZPr.

[161] § 249 odst. 2 ZPr.

[162] Včetně Obecného nařízení.

osoba, která má přístup k osobním údajům zpracovávaným správcem nebo zpracovatelem, jednala pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Evropské unie nebo členského státu. Jak již bylo výše zmíněno, správce by tedy měl svým zaměstnancům, kteří s osobními údaji pracují, podat jednoznačné pokyny, jakým způsobem s osobními údaji nakládat.[163] V důsledku toho by tedy zaměstnanci správce či zpracovatele měli být schopni rozeznat, v jaké situaci dochází k porušení zabezpečení zpracování, v jehož důsledku může vzniknout újma.

Na základě výše uvedeného lze dospět k názoru, že zaměstnanec, který má přístup k osobním údajům, má povinnost znát alespoň obecně úpravu Obecného nařízení, včetně pravidel pro náhradu újmy způsobené správcem při zpracování osobních údajů a související možnosti subjektu údajů požadovat po správci náhradu újmy. Pokud tedy dojde k porušení prevenční povinnosti a nastane hrozba vzniku škody, která je v konkrétním případě představována povinností k náhradě újmy dle Obecného nařízení, je zaměstnanec tuto skutečnost povinen nahlásit nadřízenému vedoucímu zaměstnanci.

[163] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 295.

V. NĚKTERÉ DALŠÍ ASPEKTY OBECNÉHO NAŘÍZENÍ

5.1 POVINNOST MLČENLIVOSTI ZAMĚSTNANCE SPRÁVCE A ZPRACOVATELE

5.1.1 POVINNOST MLČENLIVOSTI ZAMĚSTNANCE OBECNĚ

Jak již bylo výše zmíněno, pojem mlčenlivost není v žádném právním předpisu definován. Lze však dovodit, že povinnost mlčenlivosti spočívá v povinnosti jednat způsobem, který neumožňuje neoprávněným osobám seznámit se s informacemi, které daná osoba získala v souvislosti s výkonem své činnosti.

Zákoník práce povinnost mlčenlivosti nezakotvuje u všech zaměstnanců. Mlčenlivost o skutečnostech, o nichž se zaměstnanec dozvěděl při výkonu zaměstnání a které v zájmu zaměstnavatele nelze sdělovat jiným osobám, jsou dle § 303 odst. 2 písm. b) ZPr povinni zachovávat zaměstnanci, kteří jsou vyjmenováni v odst. 1 stejného ustanovení, tedy tzv. zaměstnanci ve veřejné správě. Co se týče všech ostatních zaměstnanců, tedy zejména zaměstnanců pracujících v soukromé sféře, není zákonná mlčenlivost ZPr výslovně zakotvena. I přes tuto skutečnost ji však z některých ustanovení ZPr je možné dovodit, jak je popsáno níže v této kapitole.

Úprava mlčenlivosti dle ZPr ovšem nijak nevylučuje ochranu obchodního tajemství obsaženou v § 2985 obč. zák. Obchodním tajemstvím jsou dle § 504 obč. zák. konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Obchodním tajemstvím tak může být například seznam zákazníků (fyzických osob), který obsahuje jejich jména, příjmení či adresy či jiné osobní údaje. Porušením obchodního tajemství je pak dle § 2985 písm. a) obč. zák. jednání, jímž jednající jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství, které může být využito v soutěži a o němž se dověděl na základě pracovního poměru.

Vzhledem k výše uvedeném lze shrnout, že povinnost zaměstnance jednat způsobem, na základě kterého nebude neoprávněným osobám umožněno seznámit se

s utajovanými informacemi je upravena jak v rovině pracovněprávní, tak občanským právem, a to nezávisle vedle sebe. Je však nutné mít na paměti, že občanskoprávní ochrana se uplatní pouze v případech, kdy daná informace bude naplňovat pojmové znaky obchodního tajemství.

5.1.2 POVINNOST MLČENLIVOSTI PODLE OchOsÚ

Zvláštní povinnost mlčenlivosti zaměstnanců je zakotvena v ustanovení § 15 OchOsÚ. Dle tohoto ustanovení jsou zaměstnanci správce, zpracovatele, ale i jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů.

Důvodem pro výslovné zakotvení povinnosti mlčenlivosti do OchOsÚ je zejména její povaha jakožto bezpečnostního prvku, který má zabránit neoprávněnému šíření osobních údajů.[164] Povinnost mlčenlivosti pomáhá zajistit, aby se s osobními údaji neseznámil neoprávněný příjemce.

Mlčenlivost je možné porušit jak způsobem aktivním, tak způsobem pasivním. K vyzrazení chráněných osobních údajů tak nemusí nutně dojít pouze jejím sdělením neoprávněné osobě, nýbrž i opomenutím, tedy např. zanecháním dokumentů obsahujícími osobní údaje či přístupová hesla k nim v místnosti bez dozoru.

Povinnost mlčenlivosti se nevztahuje pouze na samotné osobní údaje, v jejím dosahu se nachází i bezpečnostní opatření, která osobní údaje chrání. Zveřejněním těchto bezpečnostních opatření by pak mohlo dojít k získání přístupu k osobním údajům

[164] POSPÍŠIL, Daniel. § 15 [Povinnost mlčenlivosti]. In: KUČEROVÁ, Alena, NOVÁKOVÁ, Ludmila, FOLDOVÁ, Vanda, NONNEMANN, František, POSPÍŠIL, Daniel. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 248.

neoprávněnými osobami.[165] Povinnost mlčenlivosti se nevztahuje pouze na osoby, které zpracování pro správce nebo zpracovatele přímo provádějí, avšak i na další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce a zpracovatele.

Povinnost zachovávat mlčenlivost není zákonem omezena na dobu trvání pracovního poměru či jiné smlouvy a platí tak i po jejich skončení.

Jak již bylo výše uvedeno, povinnost mlčenlivosti se vztahuje vůči osobám, které nejsou oprávněny se s nimi seznámit. Z toho vyplývá, že se vztahuje zejména vůči zpřístupňování osobních údajů mimo organizaci správce nebo zpracovatele. Mlčenlivost je však nutné vnímat tak, že platí i vůči osobám fungujícím uvnitř této organizace, které se však s ohledem na své pracovní zařazení nejsou oprávněni s předmětnými informacemi seznámit. Příkladem může být povinnost mzdové účetní či nadřízených pracovníků zachovávat mlčenlivost ohledně výše platu či mzdy jiných zaměstnanců, která jim je známá.

§ 15 OchOsÚ dále uvádí, že povinností mlčenlivosti dle jeho odst. 1 není dotčena povinnost zachovávat mlčenlivost podle zvláštních zákonů, kdy příkladem může být mlčenlivost lékaře ohledně zdravotního stavu pacienta. Jednotlivé povinnosti mlčenlivosti tedy existují paralelně vedle sebe a neuplatní se zásada *lex specialis derogati legi generali.*[166]. Povinnost zachovávat mlčenlivost se rovněž nevztahuje na informační povinnost podle zvláštních zákonů.

Dle § 15 odst. 3 se povinnost mlčenlivosti nevztahuje na případy, kdy je zvláštním zákonem uložena informační povinnost. Důvodová zpráva k OchOsÚ pak uvádí, že

---

[165] NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související. Komentář.* V Praze: Wolters Kluwer, a.s., 2014, str. 241.

[166] POSPÍŠIL, Daniel. § 15 [Povinnost mlčenlivosti]. In: KUČEROVÁ, Alena, a kol. *Zákon o ochraně osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 248.

mlčenlivosti se nemůže dovolat ten, kdo má povinnost oznámit trestný čin dle trestního zákoníku.

5.1.3 POVINNOST MLČENLIVOSTI DLE NOVÉ PRÁVNÍ ÚPRAVY

Zavedením povinnosti mlčenlivosti zaměstnanců správce do českého právního řádu byly zpřísněny podmínky stanovené Směrnicí 95/46/ES, ta tuto povinnost nezakotvuje. Stejného přístupu se drží i Obecné nařízení a neobsahuje ustanovení, které by bylo obdobné ustanovení § 15 českého OchOsÚ.

Obecné nařízení se povinnosti mlčenlivosti zaměstnanců dotýká pouze okrajově, a to konkrétně v čl. 28 odst. 3 písm. b). Dle tohoto ustanovení má být zpracovateli ve smlouvě se správcem stanovena povinnost zajistit, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti. Tato povinnost však není natolik široká jako povinnost mlčenlivosti dle § 15 OchOsÚ, vzhledem k tomu, že se vztahuje pouze k zaměstnancům zpracovatele nebo k jiným osobám oprávněným provádět zpracování pro zpracovatele.

Ze znění Obecného nařízení tedy není zřejmé, zda se obecná povinnost mlčenlivosti vztahuje i na zaměstnance správce či jiné osoby oprávněné pro něj zpracování provádět, a rovněž i na osoby, které zpracování samy neprovádějí, avšak s osobními údaji přesto přicházejí do styku.

Částečnou odpověď na tuto otázku dává ustanovení § 42 návrhu zákona o zpracování osobních údajů, které ve svém aktuálním znění stejně jako § 15 OchOsÚ stanoví, že *„zaměstnanci správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a další osoby, které v rámci plnění zákonem stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce nebo zpracovatele, jsou povinni zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. Povinnost mlčenlivosti trvá i po skončení zaměstnání nebo příslušných prací“*. Je však nutné podotknout, že ustanovení § 42 návrhu zákona o zpracování osobních údajů je součástí Hlavy IV., Ochrana osobních údajů

při zajišťování obrany a bezpečnosti České republiky, a povinnost mlčenlivosti se tak použije pouze při zpracování údajů při zajišťování obrany a bezpečnosti České republiky, a nikoliv při jakémkoliv zpracování.

Povinnost mlčenlivosti osob, které s osobními údaji nakládají, zcela jistě pomáhá zajistit řádné zabezpečení osobních údajů a lze ji tak zařadit mezi jedno z bezpečnostních opatření, která by správce měl přijmout.

Ačkoliv tedy zaměstnancům povinnost mlčenlivosti nestanoví právní předpis, může tak učinit sám správce. Správce jako zaměstnavatel může povinnost mlčenlivosti se zaměstnancem sjednat v pracovní smlouvě nebo v samostatné dohodě o mlčenlivosti. Nemá však možnost povinnost mlčenlivosti uložit ve vnitřním předpisu. Důvodem pro to je znění ustanovení § 305 ZPr, jenž v odst. 1 zakazuje, aby vnitřní předpis ukládal zaměstnanci povinnosti, tedy i povinnost mlčenlivosti.[167]

Zde je však nutné zmínit i obecnou povinnost loajality zaměstnance vůči zaměstnavateli, kterou lze dovodit z ustanovení § 301 písm. d) ZPr[168], které stanoví, že zaměstnanec má povinnost nejednat v rozporu s oprávněnými zájmy zaměstnavatele a rovněž z § 249 odst. 1 ZPr, jenž zakládá zaměstnanci povinnost počínat si tak, aby nedocházelo k majetkové újmě, nemajetkové újmě ani k bezdůvodnému obohacení.

Povinnost loajality se tedy skládá z několika dílčích povinností, přičemž zahrnuje zejména povinnost zaměstnance jednat tak, aby zaměstnavateli nezpůsobil materiální

---

[167] Ke stejnému závěru dospěla na počátku roku 2016 i veřejná ochránkyně práv Anna Šabatová, přičemž dovodila, že povinnost mlčenlivosti nad rámec zákona může být sjednána pouze v pracovní smlouvě nebo jiné dohodě. Zdroj: Tisková zpráva z roku 2016, Zaměstnavatel nesmí ukládat povinnosti nad rámec zákona, dostupná na https://www.ochrance.cz/aktualne/tiskove-zpravy-2016/zamestnavatel-nesmi-ukladat-povinnosti-nad-ramec-zakona/ .

[168] BĚLINA, Miroslav. § 301 [Základní povinnosti zaměstnanců]. In: BĚLINA, Miroslav, a kol. *Zákoník práce*. 2. vydání. Praha: Nakladatelství C. H. Beck, 2015, s. 1166.

či imateriální újmu. Oprávněný zájem zaměstnavatele lze zcela jistě spatřovat ve snaze zpracovávat osobní údaje v souladu s právními předpisy a nevyzradit je neoprávněným osobám. V případě, kdy by v důsledku nesprávného jednání zaměstnance dojde k porušení některé povinnosti správce dle Obecného nařízení, vzniká správci za takové jednání odpovědnost a v konečném důsledku i škoda.

Na základě výše uvedeného se domnívám, že zaměstnanci správce vyplývá povinnost dodržovat mlčenlivost o zpracování osobních údajů i ze samotného znění ZPr. I přes tuto skutečnost se však jeví jako nejbezpečnější řešení sjednat povinnost mlčenlivosti obecně v rámci pracovní smlouvy, případně samostatné dohody o mlčenlivosti.

5.2 KODEXY CHOVÁNÍ

Skutečnost, že správce nebo zpracovatel provádí zpracování v souladu s Obecným nařízením, lze prokázat dobrovolným přihlášením se správce ke kodexu chování. Údaj o přijetí kodexu chování by pak měl být důkazem, že daný správce nejen dodržuje pravidla ochrany osobních údajů stanovená Obecným nařízením, ale může v některých případech znamenat, že správce tento obecný standard v rámci svého zpracování osobních údajů ještě dobrovolně zvýšil. Povaha, obsah a další skutečnosti s kodexy chování spojené jsou upraveny v čl. 40 Obecného nařízení.

Kodexy chování tvoří nástroje a pravidla, která se uplatňují v různých odvětvích provádějících zpracování osobních údajů a která mají za cíl přispět k řádnému uplatňování Obecného nařízení s ohledem na konkrétní povahu těchto odvětví, přičemž jejich vydávání má být podporováno jednotlivými členskými státy, dozorovými úřady, Evropským sborem a Evropskou komisí.[169] Kodexy chování tak mají mít jednotící efekt z hlediska jednotlivých odvětví, ve kterých dochází ke zpracování osobních údajů. Ačkoliv kodexy chování upravovala již Směrnice

[169] Čl. 40 odst. 1 Obecného nařízení.

95/46/ES, s jejich existencí nespojovala žádné přímé důsledky, které zavádí Obecné nařízení.[170]

Kodexy chování by měly osvětlit nejasnosti, které v různých odvětvích vznikají a měly by zohledňovat konkrétní potřeby mikropodniků a malých a středních podniků.[171] Čl. 40 v odst. 2 uvádí demonstrativní výčet oblastí, jejichž specifika v rámci daného odvětví by kodexy chování v rámci měly upřesňovat, a mezi které patří např. spravedlivé a transparentní zpracování, oprávněné zájmy, jež správci v konkrétních situacích sledují, nebo shromažďování či pseudonymizaci osobních údajů.

Dle čl. 40 odst. 5 Obecného nařízení se návrh kodexu chování nebo jeho úprava a rozšíření předkládá dozorovému úřadu. Dozorový úřad následně vydá stanovisko, zda je návrh kodexu chování v souladu s Obecným nařízením, a pokud dojde k závěru, že kodex chování poskytuje dostatečné záruky, schválí jej a následně zaregistruje a zveřejní.[172] K takto uveřejněnému kodexu následně může správce nebo zpracovatel dobrovolně přistoupit. V případě, že se návrh kodexu chování týká činností zpracování ve více členských státech, je možné předložit jej prostřednictvím Evropského sboru ke schválení Evropské komisi, která může rozhodnout o jeho všeobecné platnosti v rámci Evropské unie.[173]

---

[170] NULÍČEK, Michal a kol. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář, s. 354.

[171] Čl. 40 odst. 1 Obecného nařízení.

[172] Čl. 40 odst. 6 Obecného nařízení.

[173] Dle čl. 40 odst. 7, 8 a 9 Obecného nařízení předloží dozorový úřad návrh kodexu, který se týká činností zpracování v několika členských státech, před jeho schválením Evropskému sboru a ten vydá stanovisko k tomu, zda je návrh v souladu s Obecným nařízením. Pokud dojde k závěru, že návrh je v souladu s Obecným nařízením a poskytuje vhodné záruky, předloží Evropský sbor své stanovisko Evropské komisi. Evropská komise může prostřednictvím prováděcích aktů rozhodnout, že schválený kodex chování má všeobecnou platnost v rámci Evropské unie.

Čl. 41 Obecného nařízení pak upravuje případy, kdy dohledem nad dodržováním kodexu chování může být pověřen subjekt, který má příslušnou úroveň odborných znalostí a je pro tento účel akreditován dozorovým úřadem.

Praktický dosah schválených kodexů chování se pak projevuje v případě, kdy se správce nebo zpracovatel přihlásí k jeho dodržování. Přihlášením se k němu může správce nebo zpracovatel prokázat, že řádně plní povinností dle Obecného nařízení[174] a zavedl vhodná technická a organizační opatření pro zabezpečení zpracování.[175]

Je však nezbytné položit si otázku, jakou právní povahu a v důsledku toho i závaznost kodexy chování mají, a to zejména pro zaměstnance správce při výkonu jejich pracovní činnosti. Z povahy kodexu chování a způsobu jeho tvorby a přijímání je zřejmé, že nemá povahu obecně závazného právního předpisu. Je však zřejmé, že ačkoliv přihlášení se ke kodexu chování není povinností správce, přihlášením se k němu se správce zavazuje dodržovat jej, což mj. vyplývá i ze skutečnosti, že kodexy chování jsou dle čl. 41 monitorovány akreditovaným subjektem.

Ze skutečnosti, že se správce zaváže kodex chování dodržovat, však přímo nevyplývá, že jej jsou povinni dodržovat i jeho zaměstnanci při zpracování osobních údajů třetích osob, tedy zejména zákazníků správce. Jak již bylo zmíněno, kodex chování nemá povahu obecně závazného právního předpisu, pouhé přihlášení se správce k němu tak nezakládá povinnost zaměstnanců správce řídit se jím. Pokud má tedy správce jako zaměstnavatel v úmyslu kodexem chování zavázat i své zaměstnance, což je k jeho řádnému dodržování nepochybně nezbytné, může tento závazek promítnout do pracovní smlouvy, případně jiné zvláštní dohody, případně kodex chování přijmout v rámci své organizace jako vnitřní předpis.

[174] Čl. 24 odst. 3 Obecného nařízení, čl. 28 odst. 5 Obecného nařízení.

[175] Čl. 32 odst. 3 Obecného nařízení.

Na tomto místě je nutné poznamenat, že vnitřní předpis obecně může zaměstnanci stanovit pouze práva v pracovněprávních vztazích.[176] Vzhledem ke skutečnosti, že kodex chování rozvádí povinnosti, které jsou správci stanoveny Obecným nařízením, měl by správce v případě jeho zakotvování v rámci své organizace zvolit formu pracovního řádu.[177]

5.3 DALŠÍ ZMĚNY V PRÁVU NA OCHRANU OSOBNÍCH ÚDAJŮ

Vedle jednotlivých změn v právu na ochranu osobních údajů popsaných v předchozích kapitolách přináší Obecné nařízení i několik dalších nových povinností pro správce, a některé povinností stanovené současnou právní úpravou naopak ruší. Může se tedy zdát, že Obecné nařízení přispěje k částečnému snížení administrativní zátěže správců a zpracovatelů, v důsledku zavedení nových institutů však dojde spíše k jejímu zvýšení.

Tato část práce si dává za cíl provést pouhé shrnutí několika nových institutů, jež Obecné nařízení zavádí, a nikoli podat jejich vyčerpávající popis, a to zejména z důvodu obsáhlosti této právní úpravy.

Obecné nařízení zavádí nové právo subjektu údajů na přenositelnost osobních údajů, avšak pouze v případě, kdy se zpracování provádí automatizovaně a zároveň ke zpracování osobních údajů dochází na základě souhlasu nebo je takové zpracování nutné k plnění smlouvy, jejíž stranou je tento subjekt údajů.[178] Právo na přenositelnost spočívá v právu subjektu údajů získat zpět své osobní údaje, které správci poskytl, a to ve strukturovaném, běžně používaném a strojově čitelném formátu. Subjekt údajů má rovněž právo předat tyto údaje jinému správci, aniž by tomu původní správce bránil a také na to, aby byly jeho osobní údaje přímo předány jedním správcem jinému správci, pokud to je technicky proveditelné.

---

[176] § 305 odst. 1 ZPr.

[177] Pracovní řád dle ustanovení § 306 odst. 1 ZPr rozvádí ustanovení ZPr, popřípadě zvláštních právních předpisů podle zvláštních podmínek u zaměstnavatele, pokud jde o povinnosti zaměstnavatele a zaměstnance vyplývající z pracovněprávních vztahů.

[178] Čl. 20 Obecného nařízení.

Dílčím aspektem zásady transparentnosti, která, jak je již uvedeno výše, tvoří jednu ze základních zásad práva na ochranu osobních údajů, je dle Obecného nařízení právo subjektu údajů nebýt předmětem žádného rozhodnutí, které vychází výlučně z automatizovaného zpracování a které má pro něj právní účinky nebo se jej podobně významně dotýká.[179] Příkladem takového rozhodnutí v oblasti pracovního práva může být elektronické rozhodnutí o sankcionování či propuštění zaměstnance bez jakéhokoliv lidského zásahu. Za zmíněné automatizované zpracování lze zcela jistě považovat i profilování. Právo nebýt předmětem rozhodnutí založeného na automatizovaném zpracování se však neuplatní v případě, kdy je takové rozhodnutí nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem, pokud je povoleno právem Evropské unie nebo členského státu, nebo je založeno na výslovném souhlasu subjektu údajů.[180]

Dle čl. 30 Obecného nařízení jsou správci a zpracovatelé povinni vést písemné záznamy o zpracování osobních údajů.[181] Správce, zpracovatel, nebo jejich případní

---

[179] Čl. 22 odst. 1 Obecného nařízení.

[180] Čl. 22 odst. 2 Obecného nařízení.

[181] Záznamy správce musí dle č. 30 odst. 1 Obecného nařízení obsahovat všechny tyto informace:

a) *„jméno a kontaktní údaje správce a případného společného správce, zástupce správce a pověřence pro ochranu osobních údajů;*
b) *účely zpracování;*
c) *popis kategorií subjektů údajů a kategorií osobních údajů;*
d) *kategorie příjemců, kterým byly nebo budou osobní údaje zpřístupněny, včetně příjemců ve třetích zemích nebo mezinárodních organizacích;*
e) *informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;*
f) *je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;*
g) *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.“*

zástupci jsou pak dle odst. 4 stejného ustanovení povinni záznamy na požádání poskytnout dozorovému úřadu. Je nutné podotknout, že povinnost vést písemné záznamy se při splnění některých dalších podmínek nepoužije pro podnik nebo organizaci zaměstnávající méně než 250 osob.

Další novou povinností, kterou Obecné nařízení správcům ukládá, je posouzení vlivu zpracování na ochranu osobních údajů. Dá se říci, že tato povinnost nahrazuje doposud existující oznamovací povinnost vůči ÚOOÚ. Posouzení vlivu zpracování na ochranu osobních údajů bude správce povinen provést u takových zpracování, které mohou představovat vysoké riziko pro práva a svobody fyzických osob[182], a to zejména, pokud provádí:

a) 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 vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobě závažný dopad;
b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

---

Záznamy zpracovatele pak dle čl. 30 odst. 2 Obecného nařízení musí obsahovat:

a) *„jméno a kontaktní údaje zpracovatele nebo zpracovatelů a každého správce, pro něhož zpracovatel jedná, a případného zástupce správce nebo zpracovatele a pověřence pro ochranu osobních údajů;*
b) *kategorie zpracování prováděného pro každého ze správců;*
c) *informace o případném předání osobních údajů do třetí země nebo mezinárodní organizaci, včetně identifikace této třetí země či mezinárodní organizace, a v případě předání podle čl. 49 odst. 1 druhého pododstavce doložení vhodných záruk;*
d) *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření uvedených v čl. 32 odst. 1.“*

[182] Čl. 35 odst. 1 Obecného nařízení.

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.[183]

Dle odst. 4 a 5 stejného ustanovení má ÚOOÚ stanovit seznam operací, které budou podléhat posouzení vlivu na ochranu osobních údajů a případně může také sestavit seznam druhů operací, u nichž nebude posouzení vlivu nutné. Ke dni vypracování této práce však zatím žádná žádné takové seznamy nebyly vydány.

Posouzení vlivu na ochranu osobních údajů je postupem, jež má popsat zpracování osobních údajů, posoudit jeho nezbytnost a přiměřenost a jež má napomoci řídit rizika pro práva a povinnosti fyzických osob ze zpracování plynoucí. Zároveň má za cíl zajistit soulad zpracování s Obecným nařízením a usnadnit doložení tohoto souladu dozorovému úřadu.[184]

V případě, že správci z provedeného posouzení vlivu na ochranu osobních údajů vyplyne, že by dané zpracování mělo za následek vysoké riziko, pro jehož zmírnění správce nepřijme vhodná opatření, je povinen takové zpracování konzultovat s ÚOOÚ v rámci tzv. předchozí konzultace.[185] V případě, že ÚOOÚ dospěje k závěru, že by takové zpracování bylo v rozporu s Obecným nařízením, upozorní na to správce, přičemž může zároveň uplatnit kteroukoli ze svých vyšetřovacích, nápravných, povolovacích a poradních pravomocí.[186]

5.4 NÁSLEDKY PORUŠENÍ PRÁVA NA OCHRANU OSOBNÍCH ÚDAJŮ

Za účelem zajištění větší motivace povinných subjektů obsahuje právo na ochranu osobních právní mechanismy, kterými lze postihnout porušení z něj vyplývajících povinností. Tyto mechanismy lze dělit podle jejich povahy na mechanismy soukromoprávní, které jsou představovány povinností k náhradě újmy způsobené

[183] Čl. 35 odst. 3 Obecného nařízení.

[184] WP29 Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (*překlad vlastní*).

[185] Čl. 36 odst. 1 Obecného nařízení.

[186] Čl. 36 odst. 2 Obecného nařízení.

porušením povinnosti vyplývající z práva na ochranu osobních údajů, a mechanismy veřejnoprávní povahy, kdy se porušitel povinnosti vystavuje hrozbě postihu za přestupek, v případě vyšší škodlivosti takového jednání až za trestný čin.

5.4.1 OBECNÁ POVINNOST K NÁHRADĚ ÚJMY

Povinnost k náhradě újmy je obecně upravena v § 2894 obč. zák., který stanoví, že povinnost k náhradě nemajetkové újmy v sobě vždy zahrnuje i povinnost nahradit majetkovou škodu a že povinnost k náhradě újmy postihuje škůdce pouze v případě, kdy byla výslovně sjednána, či tak stanoví zákon.

Povinnost k náhradě majetkové škody zná rovněž OchOsÚ, který v tomto ohledu transponoval Směrnici 95/46/ES. Směrnice 95/46/ES ve svém čl. 23 stanoví, že kdo byl poškozen neoprávněným zpracováním nebo jinou činností neslučitelnou s vnitrostátními předpisy přijatými k provedení této směrnice, má právo na náhradu utrpěné škody od správce. Český zákonodárce Směrnici 95/46/ES transponoval v jejím originárním znění a čistě jazykovým výkladem by bylo možné dojít k závěru, že při porušení povinností vyplývajících z OchOsÚ má poškozený na základě OchOsÚ nárok pouze na náhradu majetkové škody. Obecné nařízení již výslovně v čl. 82 odst. 1 stanoví povinnost k náhradě jak majetkové, tak nehmotné újmy každému, kdo ji utrpěl v důsledku porušení Obecného nařízení.

Správce a zpracovatel mají možnost zprostit se odpovědnosti za porušení Obecného nařízení v případě, kdy prokáží, že nenesou žádným způsobem odpovědnost za událost, která ke vzniku újmy vedla.[187]

5.4.2 POVINNOST K NÁHRADĚ ŠKODY DLE ZÁKONÍKU PRÁCE

Zvláštní režim náhrady škody upravuje pro oblast pracovněprávních vztahů ZPr. Dle § 250 odst. 1 má zaměstnanec povinnost nahradit zaměstnavateli škodu, kterou mu způsobil zaviněným porušením povinností při plnění pracovních úkolů nebo

[187] Čl. 82 odst. 3 Obecného nařízení.

v přímé souvislosti s ním. ZPr ovšem s ohledem na základní zásadu pracovního práva zvláštní ochrany zaměstnance stanoví v § 257 odst. 2 maximální možnou výši náhrady škody, kterou je zaměstnavatel oprávněn po zaměstnanci vyžadovat, a to na čtyřapůlnásobek jeho průměrného měsíčního výdělku před porušením povinnosti, kterým způsobil škodu. Omezení výše náhrady škody se uplatní pouze v případech, kdy zaměstnanec nezpůsobil škodu úmyslně, v opilosti, nebo po zneužití jiných návykových látek.

Smyslem výše uvedeného ustanovení je ochrana příjmů zaměstnance, kdy si je zákonodárce vědom možných negativních společenských důsledků, pokud by zaměstnavatel měl možnost požadovat po zaměstnanci náhradu škody v plné výši. Ve výše uvedeném lze spatřovat rozdíl oproti úpravě náhrady škody dle Obecného nařízení, které výši náhrady škody nijak nelimituje.

Za porušení povinností vyplývajících z Obecného nařízení je dle Obecného nařízení odpovědný správce či zpracovatel. Za správce či zejména zpracovatele ovšem nelze považovat zaměstnance, který zpracování osobních údajů provádí v rámci plnění pracovních úkolů pro zaměstnavatele. I v tomto případě je nutno zohlednit povahu závislé práce, jak je upravena v § 2 odst. 2 ZPr. Předmětné ustanovení stanoví, že závislá práce je vykonávána na náklady a odpovědnost zaměstnavatele. Odpovědnost dle Obecného nařízení proto ponese zaměstnavatel, který je správcem či zpracovatelem ve smyslu Obecného nařízení. Výše uvedené přitom nijak nevylučuje možnost zaměstnavatele požadovat po zaměstnanci náhradu škody ve smyslu § 250 ZPr, která mu vznikla v důsledku poskytnutí náhrady škody subjektu údajů. V takovém případě disponuje zaměstnavatel regresním nárokem vůči zaměstnanci, při jeho uplatňování se však vždy musí řídit kogentní úpravou ZPr.

5.4.3 SPRÁVNÍ TRESTÁNÍ

Vedle povinnosti k náhradě škody, která představuje soukromoprávní důsledky porušení povinností vyplývajících z Obecného nařízení, stanoví Obecné nařízení rovněž možnosti postihu veřejnoprávní povahy cestou udělení správních pokut. Správní pokutu lze udělit pouze za porušení povinnosti a pro její uložení tak není třeba

vzniku újmy. Pokud ale taková újma vznikne, nemá uhrazení udělené pokuty vliv na povinnost takovou újmu nahradit.

Obecné principy ukládání správních pokut Obecné nařízení upravuje v čl. 83. Dle předmětného ustanovení musí být ukládání pokut v každém případě účinné, přiměřené a odrazující. Je tedy kladen důraz na preventivní funkci správních pokut, a to jak vůči osobě porušitele, tak vůči ostatním subjektům, kdy udělené pokuty musí být účinné. Zároveň je ale nutné zohlednit okolnosti daného případu a pokutu udělit ve výši těmto okolnostem přiměřené. Výčet skutečností, ke kterým je orgán udělující správní pokutu povinen při rozhodování o tom, zda pokutu uloží a případně v jaké výši, přihlédnout, stanoví Obecné nařízení ve svém čl. 83 odst. 2. Kritérii dle tohoto ustanovení je např., zda byla povinnost porušena úmyslně či z nedbalosti, zda porušitel podniknul kroky k zmírnění škody způsobených subjektu údajů, zda porušitel oznámil porušení ochrany osobních údajů dozorovému orgánu či jaké kategorie osobních údajů byly porušením dotčeny.

Obecné nařízení dále stanovuje maximální výši správních pokut, a to ve dvou úrovních. Za porušení povinností dle výčtu čl. 83 odst. 4 Obecného nařízení lze udělit pokutu až do výše 10 000 000 EUR, nebo jedná-li se o podnik, až do výše 2 % celkového ročního obratu celosvětově za předchozí finanční rok, podle toho, která hodnota je vyšší. Vyšší limit pro udělenou pokutu obsahuje čl. 83 odst. 5, kdy je na jeho základě možné udělit pokutu až do výše 20 000 000 EUR a v případech, kdy je porušitelem podnik, až do výše 4 % jeho obratu. Vyšší limitace se uplatní například v případech, kdy byly porušeny základní zásady zpracování osobních údajů. Stejně tak je vyšší sazbou možné postihnout neuposlechnutí příkazu dozorového úřadu.[188]

Obecné nařízení rovněž zakotvuje možnost členských států stanovit zvláštní postupy při ukládání správních pokut orgánům veřejné moci.[189] Návrh zákon o zpracování osobních údajů této možnosti využívá a v ustanovení § 62 stanoví maximální výši této

[188] Čl. 83 odst. 6 Obecného nařízení.

[189] Čl. 83 odst. 7 Obecného nařízení.

pokuty na 10 000 000 Kč. Tato výše pokuty je značně snížená oproti maximální výši pokuty, kterou lze uložit soukromým subjektům. V souvislosti s tím si lze položit otázku, nakolik je takové rozlišování mezi veřejnými a soukromými subjekty spravedlivé a na jakém právním základě je postaveno. Odpověď se snaží podat důvodová zpráva k návrhu zákona, která se vyjadřuje ve smyslu, že finanční prostředky orgánů veřejné moci často plynou z veřejných prostředků a by v důsledku pokutování vysokými částkami docházelo pouze k přesunům finančních prostředků v rámci státního rozpočtu.

Členské státy dále mohou na základě čl. 84 Obecného nařízení přijmout další sankce za porušení Obecného nařízení. Zavedení takových sankcí je však nutno oznámit Komisi.

ZÁVĚR

Autorka této práce si za její cíl v úvodu určila podrobnější analýzu vybraných institutů v oblasti práva ochrany osobních údajů, kdy současně upozorní na možné aplikační problémy nejen současné, ale i budoucí právní úpravy. Smyslem práce bylo rovněž poskytnout kritický rozbor nově zaváděných právních institutů a poukázat na jejich uplatnění, význam, účelnost a vhodnost. Ambicí autorky práce bylo rovněž posoudit potenciál právní úpravy obsažené v Obecném nařízení z pohledu reálného dopadu na úroveň ochrany osobních údajů.

Lze pak konstatovat, že v průběhu práce bylo upozorněno na některá možná problematická místa právní úpravy obsažené v Obecném nařízení, a to jak z důvodu nejasnosti některých použitých pojmů a formulací (např. hlavní činnost správce či rozsáhlé zpracování), tak i z důvodu logického rozporu s českým právním řádem (např. možný rozpor se zásadou nemo tenetur či možnosti postihu pověřence). Taková ustanovení se autorka pokusila opatřit komentářem, který by danou problematiku rozkryl a nabídnul řešení, či alespoň shrnul související poznatky a byl tak základem pro další úvahy.

Jedním ze stěžejních témat této práce byla analýza Obecným nařízením nově zavedeného institutu pověřence pro ochranu osobních údajů. S účinností nové právní úpravy tak budou na veřejné orgány i soukromoprávní subjekty kladeny další povinnosti, které mají přispět účinné ochraně osobních údajů. Pověřenec by měl plnit poradní a pomocnou úlohu při zpracování osobních údajů a vzhledem k jeho právním znalostem i faktickým znalostem daného oboru zvýšit úroveň ochrany osobních údajů. Ačkoli je úmysl zákonodárce ryzí, domnívám se, že kvalifikační podmínky kladené na osobu pověřence jsou nastaveny až příliš vysoko. Od pověřence je tak vyžadována nejen poměrně vysoká míra právního povědomí a znalostí práva ochrany osobních údajů, ale rovněž vhled do problematiky řízení konkrétního podniku, neboť pověřenec je povinen zajistit monitoring souladu faktického stavu s Obecným nařízením. V praxi proto bude velmi obtížné tuto funkci obsadit. Je přitom zcela zjevné, že pouze osoba disponující požadovanými vlastnostmi, která bude řádně plnit uložené povinnosti, může reálně naplnit záměr zákonodárce zvýšit standard ochrany osobních údajů.

K jasnému uchopení funkce pověřence nepřispívá ani poněkud vágní znění Obecného nařízení ohledně osob povinných funkci pověřence zřídit. Ačkoli by WP29 by v žádném případě neměla přebírat roli zákonodárce, nebylo by v daném případě na škodu vedle vypracování obecných vodítek k funkci pověřence[190] také vypracování konkrétnějšího materiálu, který by sloužil alespoň jako provizorní a částečná pomůcka pro vyhodnocení povinností subjektů, na které povinnost jmenovat pověřence potencionálně dopadá.

WP29 navíc svá sdělení a stanoviska donedávna publikovala výlučně v anglickém jazyce, kdy neoficiální překlad do českého jazyka zajišťoval pouze ÚOOÚ. Ten se navíc ukázal v několika případech chybným a ÚOOÚ za účelem odstranění nepřesností musel vydat opravený překlad. Oficiální jazykové mutace svých stanovisek začala WP29 publikovat až v nedávné době, a to ve všech úředních jazycích Evropské unie.[191] Pro úplnost autorka uvádí, že výše uvedené oficiální překlady byly zveřejněny až po vypracování vlastního obsahu této práce.

Ačkoli evropský zákonodárce zvolil pro danou úpravu v rámci zachování jednotného standartu ochrany osobních údajů formu nařízení, používání ne zcela určitých pojmů i ve zcela stěžejních případech může původní záměr znemožnit, kdy příslušné správní úřady ochrany jednotlivých členských států budou v důsledku nejednoznačnosti úpravy a absenci provádějících materiálů rozhodovat ve shodných případech rozdílně.

Problematickým se může rovněž jevit upravení významných pravidel chování pouze formou recitálů, které nemají striktně normativní povahu, namísto jejich zakomponování přímo do normativní části Obecného nařízení. Recitály zásadně nemají stanovit samotná vynutitelná pravidla chování a jejich účelem je spíše plnění interpretační funkce, kdy odhalují skutečnosti vedoucí k potřebě právní úpravy a

[190] WP29 Guidelines on Data Protection Officers (‘DPOs’).

[191] K pojmu úředního jazyka srov. Nařízení Rady č. 1 o užívání jazyků v Evropském hospodářském společenství ze dne 15. 4. 1958, ve znění pozdějších předpisů.

odůvodňují její konkrétní podobu.[192] Obecné nařízení pak na úrovni recitálů upravuje například tak důležitou otázku, jako je kontinuita platnosti souhlasu subjektu údajů se zpracováním osobních údajů.[193] Umístění tohoto pravidla pak otevírá možnosti pro polemiku ohledně jeho obecné závaznosti, což nepřispívá právní jistotě vázaných subjektů.

Poslední otázkou, na kterou se autorka pokusí zodpovědět je, zda Obecné nařízení může skutečně zlepšit úroveň ochrany osobních údajů. Je nepochybné, že při řádném dodržování stanovených pravidel dojde ke snížení možnosti zneužití osobních údajů. Na druhou stranu zpracovatelům a správcům osobních údajů mohou v důsledku zavedení institutu pověřence vzniknout nemalé finanční výdaje, a je tedy nutné v daném případě posoudit, zda je takový zásah do soukromoprávní sféry legitimní.

V současné době je Obecné nařízení určitých strašákem podnikatelů, kteří se doposud problematikou osobních údajů a jejich ochrany nezabývali, nebo tak činili pouze zevrubně. Tyto osoby pak hojně vyhledávají odbornou pomoc. Je na zvážení, zda je takovýto stav žádoucí, zejména s ohledem na situaci, kdy značnou část poptávky uspokojují ne zcela důvěryhodné podnikatelské subjekty. Ačkoli raketově rostoucí zájem o problematiku osobních údajů lze přivítat s nadšením, je nutné se pozastavit nad důvodem tohoto „boomu“, kterým dozajista nebude dobrovolný zájem a vnitřní přesvědčení o potřebnosti ochrany osobních údajů.

Diplomovou práci si dovoluji ukončit úvahou, zdali bylo za účelem zlepšení faktického stavu ochrany osobních údajů nutné přijmout nový právní předpis. Ačkoli Obecné nařízen přináší řadu nových institutů a povinností, způsob ochrany osobních údajů se mění pouze částečně. Je tedy otázkou, jestli by důsledná kontrola a vymáhání dosavadní právní úpravy nepřinesla srovnatelné, či ještě lepší výsledky. Domnívám se

[192] KLIMAS, T.; Vaiciukaite, J. (2008). *The Law of Recitals in European Community Legislation*. ILSA Journal of International Comparative Law 15(1), s. 76.

[193] Recitál 171 Obecného nařízení.

však, že činit závěry by bylo v tuto chvíli předčasné a zodpovězení otázky, zda bylo přijetí Obecného nařízení chybou nebo krokem správným směrem, ukáže až čas.

Seznam literatury a dalších zdrojů

Mezinárodní smlouvy a jiné mezinárodní dokumenty

Doporučení pro ochranu soukromí a toky osobních údajů přes hranice

Evropská úmluva o ochraně lidských práv a základních svobod

Mezinárodní pakt o hospodářských, kulturních a sociálních právech

Mezinárodní pakt o občanských a politických právech

Resolution (73) 22 on the protection of privacy of individual vis-à-vis electionic data banks in the private sector.

Resolution (74) 29 on the protection of individual vis-à-vis electionic data banks in the public sector.

Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat

Všeobecná deklarace lidských práv

Právní předpisy Evropské unie

Listina základních práv Evropské unie

Smlouva o fungování Evropské unie

Nařízení Rady č. 1 o užívání jazyků v Evropském hospodářském společenství ze dne 15. 4. 1958, ve znění pozdějších předpisů

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

Nařízení Evropského parlamentu a Rady 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislost se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES

Směrnice Evropského parlamentu a Rady 016/681 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

Směrnice Evropského parlamentu a Rady 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

Právní předpisy České republiky

Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky

Ústavní zákon č. 1/1993 Sb., Ústava České republiky

Zákon č. 582/1991 Sb., o organizaci sociálního zabezpečení, ve znění pozdějších předpisů

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, ve znění pozdějších předpisů

Zákon č. 586/1992 Sb., o daních z příjmů, ve znění pozdějších předpisů

Zákon č. 155/1995 Sb., o důchodovém pojištění, ve znění pozdějších předpisů

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání, ve znění pozdějších předpisů

Zákon č. 312/2002 Sb., o úřednících územních samosprávných celků, ve znění pozdějších předpisů

Zákon č. 480/2004 Sb., o některých službách informační společnosti, ve znění pozdějších předpisů

Zákon č. 187/2006 Sb., o nemocenském pojištění, ve znění pozdějších předpisů

Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů

Zákon č. 40/2009, trestní zákoník, ve znění pozdějších předpisů

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů

Návrh zákona o zpracování osobních údajů

Judikatura

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

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

Nález Ústavního soudu České republiky ze dne 8. listopadu 2005, sp. zn. I. ÚS 402/05

Nález Ústavního soudu České republiky ze dne 18. února 2010, sp. zn. I. ÚS 1849/08

Nález Ústavního soudu České republiky ze dne 22. března 2011, sp. zn. Pl. ÚS 24/10

Rozsudek Soudního dvoru Evropské unie ve věci C – 212/04, Konstantinos Adeneler a další v. Ellinikos Organismos Galaktos (ELOG)

Odborná literatura

BĚLINA M. a kol., Pracovní právo, 6. doplněné a podstatně přepracované vydání, Praha: C. H. Beck, 2014, 464 s., ISBN 978-80-7400-283-0

BĚLINA, M., DRÁPAL, L. a kol.: Zákoník práce. Komentář. 2. vydání. Praha: C. H. Beck, 2015, 1613 s, ISBN 978-80-7400-290-8

HENDRYCH, Dušan a kol. Správní právo. Obecná část. 9. Vydání. Praha: C.H. Beck, 2016, 600 s., ISBN: 978-80-7400-624-1

JANEČKOVÁ, E., BARTÍK, V. Ochrana osobních údajů v pracovním právu (Otázky a odpovědi). Praha: Wolters Kluwer, 2016. 192 s, ISBN 978-80-7552-145-3

KUČEROVÁ, A., NOVÁKOVÁ, L., FOLDOVÁ, V., NONNENMANN, F., POSPÍŠIL, D.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha : C. H. Beck, 2012, 536 s., ISBN 978-80-7179-226-0

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

MAŠTALKA, J.: Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 212 s., ISBN 978-80-7400-033-1

MATES, P.: Ochrana soukromí ve správním právu. 2. aktualiz. a podstatně přeprac. vyd. Praha: Linde, 2006. ISBN 80-7201-589-3

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

MORÁVEK, J.: Přehled judikatury vztahující se k právní úpravě na ochranu osobních údajů a k souvisejícím aspektům. Praha: Wolters Kluwer, a. s., 2015, s. 360, ISBN: 978-80-7552-018-0

NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů. Právní rozhledy. 2012, č. 13-14, s. 505-509

NULÍČEK, Michal a kol. GDPR - obecné nařízení o ochraně osobních údajů. Praha: Wolters Kluwer, 2017. Praktický komentář, ISBN: 978-80-7552-765-3

NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související. Komentář. V Praze: Wolters Kluwer, a.s., 2014. ISBN 978-80-7478-665-5

ŠMÍD, V. *Ochrana osobních údajů v pracovněprávních vztazích*. 2003, dostupné na http://www.fi.muni.cz/~smid/oouppv.html

Další prameny

Article 29 Data Protection Working Party, WP 136, Opinion 4/2007 on the Concept of Personal Data Adopted on 20 June 2007

Article 29 Data Protection Working Party, WP 169, Opinion 1/2010 on the Concepts of "Controller" and "Processor" Adopted on 16 February 2010

Article 29 Data Protection Working Party, WP 163, Opinion 5/2009 on Online Social Networking Adopted on 12 June 2009

Article 29 Data Protection Working Party, WP 243 rev.01, Guidelines on Data Protection Officers ('DPOs') Revised and Adopted on 5 April 2017

Article 29 Data Protection Working Party, WP 248 rev.01, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 adopted on 4 October 2017

Article 29 Data Protection Working Party, WP 250, Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017

Důvodová zpráva k Návrhu nařízení Evropského parlamentu a rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) ze dne 25. 1. 2012; zn. COM (2012) 11 final 2012/2011 (COD)

Důvodová zpráva k návrhu zákona o zpracování osobních údajů

Důvodová zpráva k zákonu č. 101/2000 Sb., sněmovní tisk 374/0

Ministerstvo vnitra České republiky, 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

Stanovisko ÚOOÚ č. 3/2011 k ochraně osobních údajů podnikajících fyzických osob

Stanovisko ÚOOÚ č. 3/2012 k pojmu osobní údaj

Stanovisko ÚOOÚ č. 4/2012 ke zpracování osobních údajů zemřelých osob

Stanovisko ÚOOÚ č. 12/2012 k použití fotografie, obrazového a zvukového záznamu osoby

Stanovisko ÚOOÚ k neoprávněnému sdružování osobních údajů nezletilých

Stanovisko ÚOOÚ k problematice odvolatelnosti souhlasu se zpracováním osobních údajů

Stanovisko ÚOOÚ k problematice aktualizace zpracovávaných osobních údajů

Tadas Klimas; Jurate Vaiciukaite, The Law of Recitals in European Community Legislation, 15 ILSA J. Int'l & Comp. L. 61, 94 (2008)

Tisková zpráva Veřejného ochránce práv z roku 2016, Zaměstnavatel nesmí ukládat povinnosti nad rámec zákona

Seznam zkratek

LZPS	Usnesení předsednictva České národní rady č. 2/1993 Sb., Listina základních práv a svobod
Obč. zák.	zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
Obecné nařízení	Nařízení Evropského parlamentu a Rady 2016/679, o ochraně fyzických osob v souvislost se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES
OchOsÚ	zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů
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
Úmluva č. 108	Úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat
ÚOOÚ	Úřad pro ochranu osobních údajů
Ústava	Ústavní zákon č. 1/1993 Sb., Ústava České republiky
WP 29	Pracovní skupina zřízená na základě čl. 29 Směrnice 95/46/ES (anglicky Article 29 Data Protection Working Party)
ZPr	Zákon č. 262/2006 Sb., zákoník práce

Abstrakt

Tato diplomová práce se skládá celkem z pěti kapitol, úvodu a závěru.

V úvodu diplomové práce se autorka věnuje uvedení do problematiky ochrany osobních údajů a jejímu významu v současném světě, kdy v něm současně vymezuje cíle práce.

V první kapitole jsou vymezeny základní prameny právní úpravy ochrany osobních údajů, a to jak na vnitrostátní, tak na evropské a mezinárodní úrovni.

Ve druhé kapitole je pozornost věnována základům právní úpravy ochrany osobních údajů, přičemž se autorka v první podkapitole věnuje vymezení základních pojmů, ve druhé podkapitole podává přehled základních principů týkajících se zpracování osobních údajů a v podkapitole třetí shrnuje právní tituly ke zpracování osobních údajů.

V kapitole třetí je rozebrán institut pověřence pro ochranu osobních údajů ve smyslu Obecného nařízení. Její první podkapitola se zabývá vymezením případů, kdy je nutné pověřence jmenovat. V druhé podkapitole se autorka věnuje problematice kvalifikačních předpokladů kladených na osobu pověřence. Tématem třetí a čtvrté podkapitoly je vymezení postavení pověřence ve vztahu ke správci a shrnutí jednotlivých úkolů stanovených pověřenci Obecným nařízením. V páté podkapitole pak autorka rozebírá jednotlivé možnosti, které může správce při jmenování pověřence zvolit a analyzuje jejich soulad s obecnými principy pracovního práva v České republice.

Čtvrtá kapitola diplomové práce se zaobírá zabezpečením osobních údajů. V její první podkapitole je rozebráno, co lze rozumět pod pojmem zabezpečení osobních údajů a jsou zde vymezeny povinnosti správce či zpracovatele, které mají za cíl eliminovat riziko zneužití osobních údajů. V podkapitole druhé je pozornost věnována institutu nově zavedenému Obecným nařízením, a to ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu. V souvislosti s tím se autorka zaměřuje i na otázku,

zda tento institut není v rozporu se základním lidským právem zákazu sebeobviňování (zásada nemo tenetur). Třetí podkapitola se rovněž týká oznamování případů porušení zabezpečení osobních údajů, avšak ve vztahu k subjektu údajů.

Poslední pátá kapitola diplomové práce je věnována dalším dopadům Obecného nařízení, zejména otázce mlčenlivosti zaměstnance správce či zpracovatele.

V závěru práce pak autorka kriticky hodnotí některé aspekty nové právní úpravy a zamýšlí se nad jejím dopadem.

Abstract

The thesis consists of five chapters, introduction and conclusion.

The author of the thesis deals with introduction to the problematics of personal data protection and its relevance in the contemporary world in the introduction of the diploma thesis as well as with demarcation of the aims of the work.

In the first chapter, the basic sources of legislation in the area of personal data protection are demarcated, both in Czech and in European and international level.

In the second chapter, the attention is paid to the basics of the legislation in the area of personal data protection, whereas the author deals with demarcation of basic concepts, in the second subchapter she gives an overview of basic principles of personal data processing and in the third subchapter she summarizes legal titles for personal data processing.

The institute of Data Protection Officer within the meaning of General Regulation is analysed in the third chapter. The first subchapter deals with demarcation of cases where the processor is obliged to designate the Data Protection Officer. The author pays attention to the problematics of requirements for qualification of the Data Protection Officer in the second subchapter. The major theme of third and fourth subchapter is demarcation of Data Protection Officers position to the controller and summarization of his individual assignments set out by the General Regulation. Further, in the fifth subchapter, the author analyses individual possible procedures of the controller in the matter of designation of Data Protection Officer and analyses their conformity with general principles of labour law in the Czech Republic.

The fourth chapter of the thesis takes a look at the security of personal data. The meaning of concept ‘security of personal data’ is analysed in the first subchapter and also the obligations of controller or processor which aim to eliminate the risk of personal data abuse are summarized here. The second subchapter pays attention to the institute of notification of a personal data breach to the supervisory authority, which is

newly brought by the General Regulation. In relation to that, the author focuses on the query whether this institute is in coherence with fundamental human right of self-incrimination prohibition (‘nemo tenetur’ principle). Third subchapter of fourth chapter regards also with notification of a personal data breach, however in the relation to the personal data subject.

The fifth and last chapter of the thesis is devoted to other aspects of the General Regulation, especially to the query of secrecy and confidentiality of the employees of the controller or processor.

The author critically evaluates some of the aspects of the new legislation and thinks about its impacts in the conclusion of the thesis.

Klíčová slova

- osobní údaj
- Nařízení GDPR
- pověřenec
- oznamování porušení zabezpečení

Keywords

- Personal Data
- GDPR
- Data Protection Officer
- Data Breach Notification

Název práce v anglickém jazyce

Problematic Aspects of Personal Data Protection