

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra práva



Diplomová práce

Zpracování osobních údajů v ČR a dopady na fyzické osoby v Armádě ČR

Petra GRUNDOVÁ

© 2019 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Petra Grundová

Veřejná správa a regionální rozvoj

Název práce

Zpracování osobních údajů v ČR a dopady na fyzické osoby v Armádě ČR

Název anglicky

Processing of personal data in the Czech Republic and impacts on natural persons in the Army of the Czech Republic

Cíle práce

Analýza platné právní úpravy ochrany a zpracování osobních údajů v ČR.

Komparace zákona č. 101/2000 Sb., o ochraně osobních údajů se zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Analýza dopadů nové právní úpravy zpracování osobních údajů v Armádě ČR (na příkladu vybraného útvaru).

Návrh změn ke zpracování osobních údajů v Armádě ČR.

Metodika

Diplomová práce bude rozdělena na dvě části, a to teoretickou a praktickou. V teoretické části bude použita metoda výkladu práva a analýza právní úpravy především se zaměřením na Nařízení Evropského parlamentu a Rady (EU) 2016/679. Komparativní metody bude použito při srovnání zákona č. 101/2000 Sb., o ochraně osobních údajů se zákonem č. 110/2019 Sb., o zpracování osobních údajů. Součástí teoretické části bude i rešerše literatury v dané oblasti. V praktické části budou analyzovány dopady nové právní úpravy zpracování osobních údajů ve vazbě na činnost Armády ČR se zřetelem k jednotlivým skupinám fyzických osob. Součástí praktické části bude kvalitativní výzkum se zaměřením na aktuální problematiku ochrany osobních údajů. Na závěr budou doporučeny změny ke zpracování osobních údajů se zaměřením na vybraný vojenský útvar.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

osobní údaj, ochrana osobních údajů, správce, subjekt údajů, zpracování osobních údajů, sankce, Úřad pro ochranu osobních údajů, Armáda České republiky.

Doporučené zdroje informací

01. BARTÍK, Václav, JANEČKOVÁ, Eva. Ochrana osobních údajů v pracovním právu (Otázky a odpovědi). Praha: Wolters Kluwer, 2016. 192 s. ISBN 978-80-7552-145-3
02. JANEČKOVÁ, Eva. GDPR. Praktická příručka implementace. Praha: Wolters Kluwer, 2018, 136 s. ISBN 978-80-7552-248-1
03. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně údajů)
04. NEZMAR, Luděk. GDPR: Praktický průvodce implementací. 1. vyd. dotisk. Praha: GRADA Publishing, a.s., 2017. 301 s. ISBN 978-80-271-0668-4
05. NOVÁK, Daniel. Zákon o ochraně osobních údajů a předpisy související. Komentář. Praha: Wolters Kluwer, 2015. 484 s. ISBN 978-80-7478-665-5
06. Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, ve znění pozdějších předpisů
07. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
08. ŽŮREK, Jiří. GDPR v personalistice. 1. vyd. Olomouc: ANAG, 2019. 176 s. ISBN 978-80-7554-210-6
09. ŽŮREK, Jiří. Praktický průvodce GDPR. 1. vyd. dotisk. Olomouc: ANAG, 2017. 223 s. ISBN 978-80-7554-097-3
10. Zároveň další literatura podle pokynů vedoucí práce

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

JUDr. Jitka Mráčková, CSc.

Garantující pracoviště

Katedra práva

Elektronicky schváleno dne 24. 11. 2017

JUDr. Jana Borská, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 24. 11. 2017

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 18. 11. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Zpracování osobních údajů v ČR a dopady na fyzické osoby v Armádě ČR" jsem vypracovala samostatně pod vedením vedoucí diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 23. listopadu 2019

Poděkování

Ráda bych touto cestou poděkovala JUDr. Jitce Mráčkové CSc. za vedení práce a veškerou pomoc při psaní.

Zpracování osobních údajů v ČR a dopady na fyzické osoby v Armádě ČR

Souhrn

Diplomová práce se zabývá problematikou ochrany a zpracování osobních údajů se zaměřením na Armádu České republiky (AČR). Teoretická část se věnuje analýze právní úpravy ochrany a zpracování osobních údajů v ČR (zákon č. 101/2000 Sb., o ochraně osobních údajů, zákon č. 110/2019 Sb., o zpracování osobních údajů a Nařízení Evropského parlamentu a Rady (EU) 2016/679). Pozornost je také věnována vývoji sankcí v příslušné právní úpravě. V praktické části jsou analyzovány dopady nové právní úpravy zpracování osobních údajů v AČR a její vliv na běžnou činnost u konkrétního vojenského útvaru. Součástí diplomové práce je kvalitativní výzkum se zaměřením na aktuální problematiku ochrany a zpracování osobních údajů. V závěru práce jsou doporučeny změny ke zpracování osobních údajů u vybraného vojenského útvaru.

Klíčová slova: osobní údaj, ochrana osobních údajů, správce, subjekt údajů, zpracování osobních údajů, sankce, Úřad pro ochranu osobních údajů, Armáda České republiky.

Processing of personal data in the Czech Republic and impacts on natural persons in the Army of the Czech Republic

Summary

This thesis deals with the issue of protection and processing of personal data with a focus on the Army of the Czech Republic (ACR). The theoretical part is devoted to the analysis of legal regulations of the protection and processing of personal data in the Czech Republic (Act No. 101/2000 Coll., On the protection of personal data, Act No. 110/2019 Coll., On the processing of personal data and Regulation (EU) 2016/679 of the European Parliament and of the Council). Attention is also paid to the development of sanctions in the relevant legislation. The practical part analyzes the impact of the new legislation on the processing of personal data in the Army of the Czech Republic and its impact on routine activities of a specific military unit. Part of the thesis is a qualitative research focusing on current issues of protection and processing of personal data. At the end of the work are recommended changes to the processing of personal data for the selected military unit.

Keywords: personal data, personal data protection, controller, data subject, personal data processing, sanctions, Office for Personal Data Protection, Army of the Czech Republic

3.4.1.2	Posun v novém zákoně o zpracování osobních údajů	36
3.4.1.3	Volba orgánu příslušného k akreditaci certifikačních těles.....	37
3.4.1.4	Ustavení nezávislého dozorového orgánu, zajištění jeho činnosti, procedura jmenování jeho vedení, zajištění nezávislosti vedení i zaměstnanců ..	37
3.4.1.5	Případné doplňující sankce za porušení ochrany osobních údajů (kromě dosud existujících).....	38
3.4.1.6	Vyvážení svobody projevu a ochrany osobních údajů.....	39
3.4.2	Shrnutí	40
4	Praktická část.....	41
4.1	Zaměření na konkrétní útvar AČR.....	41
4.1.1	Ozbrojené síly České republiky	41
4.1.2	Armáda České republiky	42
4.1.3	41. mechanizovaný prapor v Žatci.....	45
4.1.3.1	Historie vzniku útvaru.....	45
4.1.3.2	Současnost	46
4.1.3.3	Ochrana osobních údajů u 41. mpr před nabytím účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679.....	47
4.1.4	Shrnutí	49
4.2	Nařízení Evropského parlamentu a Rady (EU) 2016/679 v AČR, s konkrétním zaměřením na 41. mpr.....	50
4.2.1	Promítnutí Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracovávání osobních údajů v AČR.....	50
4.2.1.1	Promítnutí základních pojmů Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracování osobních údajů	53
4.2.1.2	Dodržování zásad zpracování osobních údajů.....	57
4.2.1.3	Posouzení vlivu na ochranu osobních údajů	60
4.2.1.4	Zajišťování ochrany osobních údajů	60
4.2.1.5	Povinnosti při zjištění porušení zabezpečení osobních údajů	61
4.2.1.6	Povinnosti správce vůči subjektu údajů	63
4.2.2	Promítnutí Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracovávání osobních údajů u 41. mpr.....	65
4.2.2.1	Promítnutí základních pojmů Nařízení Evropského parlamentu a Rady (EU) 2016/679 do činnosti 41. mpr	65
4.2.2.2	Vliv na běžnou činnost 41. mpr	66
4.2.3	Shrnutí	68
4.3	Zpracování osobních údajů před a po nabytí účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679 u 41. mpr	70

4.3.1	Úvodem	70
4.3.2	Řízené rozhovory	72
4.3.3	Zpracování osobních údajů před nabytím účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679	73
4.3.3.1	Zpracování osobních údajů souvisejících s příchodem fyzických osob k útvaru	73
4.3.3.2	Zpracování osobních údajů souvisejících s průběhem služebního/pracovního poměru fyzických osob	76
4.3.3.3	Zpracování osobních údajů souvisejících s odchodem fyzických osob od útvaru	77
4.3.3.4	Shrnutí	78
4.3.4	Zpracování osobních údajů po nabytí účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679	80
4.3.4.1	Zpracování osobních údajů souvisejících s příchodem fyzických osob k útvaru	80
4.3.4.2	Zpracování osobních údajů souvisejících s průběhem služebního/pracovního poměru fyzických osob	81
4.3.4.3	Zpracování osobních údajů souvisejících s odchodem fyzických osob od útvaru	84
4.3.4.4	Shrnutí	85
4.4	Zhodnocení výsledků a doporučení	86
4.4.1	Zhodnocení výsledků a doporučení ke zpracování osobních údajů v AČR..	86
4.4.2	Zhodnocení výsledků a doporučení ke zpracování osobních údajů u 41. mpr	87
5	Výsledky a diskuze	90
5.1	K vývoji právní úpravy v oblasti ochrany a zpracování osobních údajů	90
5.2	K implementaci Obecného nařízení 2016/679 u 41. mpr	91
5.3	K povinnostem zaměstnanců 41. mpr při zpracovávání osobních údajů	92
5.4	K bezpečnostním opatřením při zpracování osobních údajů u 41. mpr	93
5.5	K povinnostem při zjištění případů porušení zabezpečení osobních údajů	94
6	Závěr	96
7	Seznam použitých zdrojů	98
7.1	Prameny mezinárodního a evropského práva	98
7.2	Právní předpisy	98
7.3	Vnitřní předpisy	100
7.4	Tištěná literatura	100
7.5	Elektronické dokumenty	101

8 Přílohy	103
8.1 Příloha A Posouzení vlivu na ochranu osobních údajů	103
8.1.1 Účel zpracování osobních údajů	104
8.1.2 Právní základ zpracování osobních údajů	106
8.1.3 Rozsah zpracovaných osobních údajů.....	108
8.1.4 Posouzení rizik hrozících subjektu údajů z procesu zpracování osobních údajů	108
8.1.5 Stanovení předběžných organizačních a technických opatření	110
8.1.6 Zpráva o posouzení vlivu na ochranu osobních údajů	111
8.2 Příloha B Jmenovitá evidence.....	113
8.3 Příloha C Prohlášení MO o zpracování osobních údajů.....	115
8.4 Příloha D Upřesnění práce s osobními údaji v účetních evidencích FIS	118
8.5 Příloha E Poučení o zpracování osobních údajů o.z. před nabytím účinnosti Obecného nařízení 2016/679	121
8.6 Příloha F Souhlas s využitím kontaktních údajů o.z. před nabytím účinnosti Obecného nařízení 2016/679.....	123
8.7 Příloha G Souhlas se zpracováním osobních údajů po skončení pracovního poměru o.z. před nabytím účinnosti Obecného nařízení 2016/679	124
8.8 Příloha H Poučení o zpracování osobních údajů o.z. po nabytí účinnosti Obecného nařízení 2016/679.....	125
8.9 Příloha I Souhlas se zpřístupněním osobních údajů nad rámec zákonného povolení po nabytí účinnosti Obecného nařízení 2016/679	127
8.10 Příloha J Souhlas se zpracováním osobních údajů po skončení pracovního poměru o.z. po nabytí účinnosti Obecného nařízení 2016/679	128
8.11 Příloha K Otázky pro řízený rozhovor	130

Seznam obrázků

Obrázek 1 Struktura ozbrojených sil České republiky	42
Obrázek 2 Členění pozemních sil AČR.....	43
Obrázek 3 Členění vzdušných sil AČR.....	44
Obrázek 4 Struktura 41. mechanizovaného praporu	46
Obrázek 5 Grafické znázornění nastavení práv a povinností dle RMO č. 16/2013	51
Obrázek 6 Schéma přímo podřízených ministrovi obrany	69
Obrázek 7 Základní rozdělení personální evidence	71
Obrázek 8 Členění osobního spisu	76
Obrázek 9 Rozsáhlost pokrytí sociální sítě Facebook.....	83
Obrázek 10 Schéma analýzy rizik.....	109

Seznam grafů

Graf 1 Nárůst uživatelů sociální sítě Facebook	83
--	----

Seznam tabulek

Tabulka 1 Vývoj formulace požadavků při zpracování osobních údajů	19
Tabulka 2 Propojení článků a recitálů Obecného nařízení 2016/679.....	25
Tabulka 3 Postihy při neoprávněném nakládání s osobními údaji.....	29
Tabulka 4 Postihy za šíření pomluvy	29
Tabulka 5 Sankce za přestupky fyzických osob	30
Tabulka 6 Sankce za správní delikty právnických osob.....	31
Tabulka 7 Porušení povinností odpovídající pokutě do výše 10 000 000 EUR	32
Tabulka 8 Porušení povinností odpovídající pokutě do výše 20 000 000 EUR	33
Tabulka 9 Rozdíl mezi osobním, anonymním a pseudonymizovaným údajem	56
Tabulka 10 Zásady zpracování osobních údajů	59
Tabulka 11 Zpracovávané osobní údaje fyzických osob v jednotlivých fázích poměru.....	70
Tabulka 12 Číselná evidence	72
Tabulka 13 Zákonné oprávnění ke zpracovávání osobních údajů u jednotlivých kategorií fyzických osob	74
Tabulka 14 Přehled personální evidence u jednotlivých kategorií fyzických osob	79
Tabulka 15 Nejčastěji používaná hesla v ČR	82
Tabulka 16 Rozsah a účel zpracování osobních údajů v rezortu MO	105
Tabulka 17 Členění jmenovité evidence	113

1 Úvod

Prudký technologický rozmach a rozvoj internetu posledních let s sebou přinesl vyšší riziko a nebezpečí pro soukromí každého z nás. Rozsah zpracovávaných informací, kamerové systémy, jakožto součást našich každodenních životů, sdílení informací napříč celým světem, to vše jsou výdobytky moderní doby. Stinnou stránkou tohoto technologického rozmachu je ovšem zvýšené nebezpečí ztráty našeho základního práva, a to práva na ochranu osobních údajů při jejich zpracování.

Na základě rozrůstající se problematiky ochrany osobních údajů přestávala být doposud platná legislativa dostačující a bylo nutné situaci adekvátně řešit. Po zkušenostech se Směrnicí 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, která harmonizaci zabezpečila jen v základních otázkách a částečně, bylo nově pro revizi právního rámce zpracování osobních údajů použito nařízení Evropské unie.¹

Výhodou Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES jsou pravidla přímo aplikovatelná na adresáty ve všech státech Evropské unie, což ho činí v tomto ohledu revolučním. Ruku v ruce s novým právním rámcem, řešícím zpracování osobních údajů, dochází k přijetí Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV a dále Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Pro potřeby této práce bude pozornost prioritně zaměřena na první z trojice evropských právních předpisů.

K upřesnění nových principů a povinností, vyplývajících z evropského nařízení, dochází v České republice dne 24. dubna 2019 k vyhlášení zákona č. 110/2019 Sb., o zpracování osobních údajů, jakožto náhrady za doposud platný zákon č. 101/2000 Sb.,

¹ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 15.

o ochraně osobních údajů. Společně se zákonem č. 110/2019 Sb. vstupuje v platnost také doprovodný právní předpis, a to zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.

Teoretická část bude složena ze čtyř kapitol. První bude zaměřena na historii právní úpravy ochrany a zpracování osobních údajů. Druhá kapitola bude zaměřena na předpisy Evropského práva v oblasti ochrany a zpracování osobních údajů. Třetí kapitola se bude věnovat vývoji sankcí v právní úpravě, počínaje zákonem č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, až po současně platnou legislativu, tedy zákon č. 110/2019 Sb., o zpracování osobních údajů. Poslední kapitola teoretické části se bude zabývat komparací zákona č. 101/2000 Sb. se zákonem č. 110/2019 Sb. se zaměřením na nový přístup k osobním údajům.

V praktické části budou analyzovány dopady nové právní úpravy zpracování osobních údajů ve vazbě na činnost Armády ČR se zřetelem k jednotlivým skupinám fyzických osob. Důraz bude kladen na jednotlivé fáze služebního/pracovního poměru fyzických osob a s tím souvisejícím zpracováním jejich osobních údajů. Získané teoretické poznatky budou následně aplikovány na konkrétní vojenský útvar a jeho běžnou činnost. Pomocí výstupů z kvalitativního výzkumu budou snadněji pochopeny základní principy zpracování osobních údajů při běžné činnosti u vybraného vojenského útvaru.

Komparací poznatků ohledně běžné činnosti u Armády ČR, získaná před a po nabytí účinnosti evropské právní úpravy a na základě kvalitativního výzkumu, bude analyzována běžná činnost při zpracování osobních údajů. Dalšími očekávanými výstupy této práce jsou doporučení ke zlepšení ochrany osobních údajů fyzických osob při jejich zpracování. Přestože se jedná o analýzu stavu jednoho vojenského útvaru, zevšeobecněné výstupy a návrhy lze aplikovat na jakýkoliv vojenský útvar v Armádě České republiky.

2 Cíl práce a metodika

2.1 Cíl práce

Tato práce si klade za cíl analyzovat právní úpravu ochrany a zpracování osobních údajů v České republice. Následně chce srovnat zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ve znění pozdějších předpisů se zákonem č. 110/2019 Sb., o zpracování osobních údajů. Dále na příkladu vybraného útvaru Armády ČR analyzuje dopady Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „Obecné nařízení 2016/679“) a navrhuje změny ke zpracování osobních údajů v Armádě ČR.

Mezi dílčí cíle teoretické části patří analýza historického vývoje právní úpravy v oblasti ochrany a zpracování osobních údajů se zaměřením na vybrané otázky zákona č. 101/2000 Sb., o ochraně osobních údajů. Navazuje analýza předpisů Evropského práva v oblasti ochrany a zpracování osobních údajů. Dalším cílem je zmapování problematiky vývoje sankcí v právní úpravě ve veřejném právu a následná komparace zákona č. 101/2000 Sb., o ochraně osobních údajů s novými přístupy v této oblasti. Syntézou těchto poznatků dochází k definování změn v nové právní úpravě, a to v zákoně č. 110/2019 Sb., o zpracování osobních údajů.

Cílem praktické části je, na základě promítnutí Obecného nařízení 2016/679 do problematiky zpracování osobních údajů v Armádě ČR (s konkrétním zaměřením na vybraný útvar), analyzovat dopady na fyzické osoby a navrhnout doporučení ke zlepšení ochrany jejich osobních údajů při zpracování.

2.2 Metodika

V teoretické části je provedena analýza právní úpravy především se zaměřením na Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Dále je v uvedené oblasti použita metoda výkladu práva. Komparativní metodou bude postupováno při srovnání zákona č. 101/2000 Sb., o ochraně osobních údajů se zákonem č. 110/2019 Sb., o zpracování osobních údajů. Komparativní metoda bude dále použita při srovnání vývoje sankcí v právní úpravě, a to od nabytí účinnosti zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech až po platnou právní úpravu. Nedílnou součástí teoretické části je i rešerše literatury v dané oblasti.

V praktické části je nejprve analyzován stav ochrany osobních údajů u vybraného vojenského útvaru Armády ČR před nabytím účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679. Následuje analýza stavu zpracovávání osobních údajů po aplikaci nové evropské právní úpravy a její promítnutí do praxe Armády ČR.

Na základě zpracování zjištěných dat a za použití kvalitativního výzkumu, konkrétně řízených rozhovorů s vedoucími pracovníky vybraného vojenského útvaru, jsou analyzovány procesy zpracovávání osobních údajů v jednotlivých fázích služebního/pracovního poměru fyzických osob v Armádě ČR, a to před i po nabytí účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679.

S využitím syntézy zjištěných informací jsou navržena doporučení ke zpracovávání osobních údajů jak v Armádě ČR, tak u konkrétního vojenského útvaru.

3 Teoretická část

3.1 Historie právní úpravy ochrany a zpracování osobních údajů

3.1.1 Úvod do problematiky

Historicky prvním mezinárodním dokumentem zaručujícím právo na soukromí byla Všeobecná deklarace lidských práv, která byla schválena Valným shromážděním Organizace spojených národů 10. prosince 1948. Konkrétně čl. 12 deklaruje, že „*nikdo nesmí být vystaven svévolnému zasahování do soukromého života*“ a dále, že „*každý má právo na zákonnou ochranu proti takovým zásahům*.“² Tento dokument se stal inspirací pro Radu Evropy, která v roce 1950 sjednala Evropskou úmluvu o ochraně lidských práv a základních svobod a v článku 8³ specifikovala právo na respektování soukromého a rodinného života. Tyto dva mezinárodní dokumenty sice deklarovaly právo na soukromí pouze obecně, ale nezabývaly se ochranou osobních údajů při jejich zpracování. Z důvodu rozvoje společnosti a souvisejícím vývojem automatizovaných prostředků, sloužícím ke zpracování osobních dat, se výše zmíněné mezinárodní dokumenty postupem času staly nedostačujícími. Nutností bylo „*na tuto skutečnost speciálně reagovat a de facto začít chápat ochranu osobních údajů při jejich zpracování jako samostatnou právní oblast zasluhující zvláštní právní pozornost*.“⁴

3.1.2 Předrevoluční období

Za prototypový dokument, deklarující cíle a ambice ochrany osobních údajů a zároveň zahrnující i jejich zpracování, lze považovat Úmluvu Rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat (dále jen „Úmluva č. 108/1981“). Účelem tohoto dokumentu je zaručení každé fyzické osobě na území každé smluvní strany úctu k jejím právům a základním svobodám a zejména k jejím právům na soukromý život se zřetelem na automatizované zpracování osobních údajů, které

² *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.* Viz čl. 12 Všeobecné deklarace lidských práv.

³ (1) *Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.*
(2) *Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.* Viz čl. 8 Evropské úmluvy o ochraně lidských práv.

⁴ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 13.

se k ní vztahují.⁵ K přijetí tohoto dokumentu došlo dne 28. ledna 1981 a mělo tak zásadní dopad na problematiku osobních údajů, že v současnosti je 28. leden považován za Mezinárodní den ochrany osobních údajů.⁶

Českou republikou byla Úmluva č. 108/1981 podepsána až v září roku 2000, čímž byla zahájena její ratifikace. Z důvodu nesouladu s naší legislativou došlo k definitivnímu souhlasu být vázán touto mezinárodní smlouvou až v červenci 2001 (Sdělení č. 115/2001 Sb. m. s.). Úmluva č. 108/1981 poprvé definovala termíny jako osobní údaj, správce, automatizované zpracování, vymezila zvláštní skupiny údajů, zásady zpracování osobních údajů či nutnost údaje zabezpečit. „*Definice osobního údaje po obsahové stránce přetrvává dodnes a nic na ni nemění ani Obecné nařízení.*“⁷ Stejně tak nebylo nutné po obsahové stránce měnit pojmy správce či zpracovatel. Úmluva č. 108/1981 kladla důraz na kvalitu údajů a na jejich poctivé získávání, zpracování a řádné zabezpečení. „*Úmluvou č. 108 byly položeny základy ochrany osobních údajů při jejich zpracování, na kterých stavěly další evropské dokumenty.*“⁸

3.1.3 Porevoluční období

Z důvodu rychlého vývoje společnosti, automatizace a počínající globalizace v 80. a 90. letech 20. století vyvstala nutnost určitým způsobem sjednotit pravidla ochrany osobních údajů. Vlivem volného pohybu osob, zboží a služeb v evropském prostoru docházelo i k pohybu osobních údajů, a tím vycházelo najevo, že dílčí vnitrostátní právní úpravy přestávají být dostatečné.

Vyústěním snahy o sjednocení právní úpravy ochrany osobních dat v evropském prostoru z důvodu neustálého technologického vývoje bylo schválení Směrnice⁹ Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů (dále jen „Směrnice 95/46/ES“), jakožto právního předpisu navazujícího na Úmluvu č. 108/1981. V mnohém se Úmluvou č. 108/1981 inspirovala (viz Tabulka 1), ale nově se nezaměřovala

⁵ MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2008, s. 2.

⁶ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 14.

⁷ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 13.

⁸ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 14.

⁹ Směrnice stanovuje členskými státy Evropské unie, čeho mají dosáhnout ve svých vnitrostátních rádech.

pouze na částečně či plně automatizované zpracování, nýbrž i na neautomatizované zpracování osobních údajů.¹⁰

Tabulka 1 Vývoj formulace požadavků při zpracování osobních údajů

Úmluva č. 108/1981	Směrnice 95/46/ES
Osobní údaje musí být:	
získány a zpracovány poctivě a v souladu se zákony;	zpracovány korektně a přípustným způsobem;
shromažďovány pro stanovené a oprávněné účely a nesmí jich být použito způsobem neslučitelným s těmito účely;	sbírány pro stanovené účely, výslovně vyjádřené a legitimní a nesmí být dodatečně zpracovávány způsobem neslučitelným s těmito účely;
přiměřené, týkající se účelů, pro něž byly uloženy na nosiče, a nepřesahující tyto účely;	přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou sbírány a pro které jsou dodatečně zpracovávány;
přesné, a pokud je to potřebné, udržované v aktuálním stavu;	přesné, a je-li to nezbytné, i aktualizované;
uchovávány ve formě umožňující zjistit totožnost subjektů údajů po dobu nikoli delší, než je třeba pro účely, pro něž jsou údaje shromažďovány.	zachovány ve formě umožňující identifikaci osob po dobu nepřesahující období nezbytné pro uskutečnění cílů, pro které jsou sbírány nebo dodatečně zpracovávány.

Zdroj: zpracováno dle MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2008, s. 4 a 5.

Hlavním rozdílem mezi uvedenými dokumenty bylo, že Směrnice 95/46/ES pojala zpracování osobních údajů komplexně a nově „*upravovala rovněž aspekty předávání osobních údajů nejen do zemí Evropské unie, ale i mimo ně.*“¹¹

Pro směrnici, jakožto právní akt Evropské unie, je charakterizující její harmonizační účinek na právní řády jednotlivých členských zemí Evropské unie, práva a povinnosti subjektům vnitrostátního práva však nestanovuje přímo. Jednotlivým členským státům tedy vznikla povinnost přijmout adekvátní právní předpisy, avšak některé státy si její provedení vysvětlovaly různými způsoby. Výsledkem toho bylo, že jednotlivé vnitrostátní právní úpravy se od sebe začaly postupem času výrazně lišit a požadovaná harmonie byla výrazně narušena.¹²

¹⁰ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 14.

¹¹ Tamtéž, s. 14.

¹² Tamtéž, s. 15.

3.1.4 K vybraným otázkám zákona č. 101/2000 Sb., o ochraně osobních údajů

V České republice se s pojmy souvisejícími s ochranou informací respektive osobních údajů setkáváme v roce 1991, kdy došlo k ústavní úpravě práva na soukromí, práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobě. Tato úprava byla zakotvena v čl. 10¹³ v Listině základních práv a svobod, vyhlášené ústavním zákonem č. 23/1991 Sb. a republikované usnesením předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky ve znění zákona č. 162/1998 Sb. (dále jen „Listina“). Zkráceně lze tato práva nazvat jako „práva na ochranu osobních údajů“. Do pomyslné opozice vůči právu na ochranu osobních údajů lze postavit „právo na informace“, které je zakotveno v čl. 17 Listiny¹⁴ a mimo jiné zahrnuje ustanovení, která zaručují každému právo „svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu“. Z teoretického hlediska se ovšem obě výše uvedená práva podobají, neboť jsou shodně nástrojem kontroly moci, s cílem ochránit jednotlivce proti rušivým zásahům aktivně konajících státních a soukromých činitelů.¹⁵

Se samostatným řešením problematiky ochrany osobních údajů při jejich zpracování se v České republice setkáváme až s přijetím zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech (dále jen „zákon č. 256/1992 Sb.“). Tato zákonná úprava definovala základní pojmy a vymezila hlavní zásady nakládání s osobními údaji včetně povinností, které byly s nakládáním spojeny. Jednalo se především o povinnosti provozovatelů takových informačních systémů a dále fyzických a právnických osob provádějících činnost v souvislosti s provozem informačních systémů. Po rozpadu České a Slovenské Federativní Republiky došlo k převzetí zákona Českou republikou, v praxi

¹³ (1) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(2) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Viz čl. 10 Listiny základních práv a svobod.

¹⁴ (1) Svoboda projevu a právo na informace jsou zaručeny.

(2) Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem, jakož i svobodně vyhledávat, přijímat a rozšiřovat ideje a informace bez ohledu na hranice státu.

(3) Cenzura je nepřípustná.

(4) Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti.

(5) Státní orgány a orgány územní samosprávy jsou povinny přiměřeným způsobem poskytovat informace o své činnosti. Podmínky a provedení stanoví zákon. Viz čl. 17 Listiny základních práv a svobod.

¹⁵ MATOUŠOVÁ, M., HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2008, s. 7.

ovšem nebyl realizován. Důvodem byl fakt, že v zákoně nebylo obsaženo manuální zpracování osobních údajů, úprava sankcí pro případ jeho porušení, ani ustanovení o zřízení nezávislého dozorového orgánu. Výsledkem nedostatečné právní úpravy byla v 90. letech minimální informovanost veřejnosti o právní úpravě ochrany osobních údajů a s tím související možnost hájit svá práva.¹⁶

Z důvodu nedostatečné právní ochrany osobních údajů byla Česká republika terčem kritiky ze strany Evropské unie. Jelikož se ČR ucházela o její členství, bylo nutné přijmout adekvátní právní úpravu pro zabezpečení kompatibility s předpisy Evropské unie. Nastala situace vedla k přijetí zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů ve znění pozdějších předpisů (dále jen „zákon č. 101/2000 Sb.“). Přijetí toho zákona znamenalo výrazný zlom v oblasti ochrany osobních údajů. Spolu s jeho zavedením do našeho právního řádu došlo k posílení postavení jednotlivce jako subjektu údajů a zaručení jisté ochrany před neoprávněnými zásahy do jeho soukromí. Nově zavedl termíny, jejichž užití bylo žádoucí již v minulosti, a také byl schopen rozlišit automatizované a neautomatizované zpracování osobních údajů.

Zákon č. 101/2000 Sb. nově zřídil Úřad pro ochranu osobních údajů¹⁷ (dále jen „ÚOOÚ“), dále specifikoval práva a povinnosti při zpracování či likvidaci osobních údajů, oznamovací povinnosti a také podmínky přenosu osobních údajů do zahraničí. Definoval základní pojmy problematiky ochrany osobních údajů a prostřednictvím novelizací pružně reagoval na nové změny v souladu s mezinárodními dokumenty. Že se jedná o problematiku stále se vyvíjející, svědčí i fakt, že byl zákon č. 101/2000 Sb. osobních údajů 24krát novelizován.¹⁸ K nejvýznamnější novelizaci došlo v roce 2004 z důvodu realizace Směrnice 95/46/ES na zákonné úrovni.¹⁹

Právní předpisy, které upravují ochranu osobních údajů při jejich zpracování, částečně zahrnují i ochranu soukromí. Ochrana soukromí v nejširším slova smyslu

¹⁶ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 18.

¹⁷ Úřad pro ochranu osobních údajů vykonává působnost dozorového orgánu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu. Viz § 2 odst. 3 zákona č. 101/2000 Sb., o ochraně osobních údajů.

¹⁸ Zákony č. 227/2000 Sb., č. 177/2001 Sb., č. 450/2001 Sb., č. 107/2002 Sb., č. 310/2002 Sb., č. 517/2002 Sb., č. 439/2004 Sb., č. 480/2004 Sb., č. 439/2004 Sb., č. 626/2004 Sb., č. 413/2005 Sb., č. 444/2005 Sb., č. 342/2006 Sb., č. 109/2006 Sb., č. 170/2007 Sb., č. 52/2009 Sb., č. 41/2009 Sb., č. 227/2009 Sb., č. 281/2009 Sb., č. 468/2011 Sb., č. 375/2011 Sb., č. 64/2014 Sb., č. 250/2014 Sb., č. 301/2016 Sb.

¹⁹ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 19.

je ovšem upravena zákonem č. 89/2012 Sb., občanský zákoník, a to § 81 odst. 2²⁰. I přesto, že občanský zákoník zahrnuje především zásady ochrany soukromí u jednání, které není zpracováním osobních údajů, lze ho uplatnit v případech, „*kdy komukoliv vznikne hmotná či nehmotná újma způsobená zpracováním osobních údajů. Tuto škodu lze v intencích občanského zákoníku nárokovat prostřednictvím procesních ustanovení u soudu.*“²¹

3.1.5 Shrnutí

Právo na ochranu osobních údajů, původně součást práva na soukromí, se ve větší míře začalo řešit až na počátku 20. století. Jeho význam narůstal přímou úměrou, a to především z důvodu rostoucí potřeby chránit soukromí jednotlivců v souvislosti s rozvojem komunikačních a informačních technologií. Zájem o právo na ochranu osobních údajů nebyl pouze v gesci jednotlivých států, ale po 2. světové válce se stal tématem řešeným na mezinárodní úrovni. Prvním ze zásadních mezinárodních dokumentů byla Všeobecná deklarace lidských práv zabývající se jak právem na ochranu soukromí, tak ochranou osobních údajů. Na základě inspirace od OSN přijala Rada Evropy o dva roky později další lidsko-právní dokument - Evropskou úmluvu o ochraně lidských práv a svobod.

Snaha o mezinárodní závazný dokument zabývající se výhradně ochranou osobních údajů vyústila v roce 1980, kdy Rada Evropy přijala Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních údajů. I přesto, že se dokument zaměřoval pouze na specifickou výseč celé problematiky ochrany osobních údajů, většina dokumentů přijatých v následujících letech v něm hledala inspiraci. Za jeden z těchto dokumentů lze chápat Směrnici 95/46/ES, která nově zohlednila i problematiku neautomatizovaného zpracování osobních dat.

V České republice byl vlivem totalitního režimu a nezájmu politiků řešit problematiku ochrany osobních údajů vývoj právní úpravy značně opožděn oproti vývoji evropskému. V době komunistického režimu byla řešena pouze ochrana osobnosti, a to dle

²⁰ *Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy. Viz § 81 odst. 2 zákona č. 89/2012 Sb., občanský zákoník.*

²¹ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 20.

§ 11 zákona č. 40/1964 Sb., občanský zákoník²². První ustanovení zahrnující přímo právo na ochranu osobních údajů přichází až po revoluci, konkrétně v zákoně č. 256/1992 Sb. Přijetí zmiňovaného zákona lze chápat jako snahu o určitý druh ochrany na základě zkušeností zažitých během listopadové revoluce.²³ Nedostatkem této právní úpravy ovšem byla především zaměřenost na osobní údaje v informačních systémech, nedostatečné ustanovení ohledně sankcí a v neposlední řadě absence ustanovení týkající se zřízení dozorového orgánu.

Snaha České republiky o členství v Evropské unii byla určitým „motorem“ k zajištění kompatibility české právní úpravy s evropskou. Vyústěním snahy bylo přijetí zákona č. 101/2000 Sb., který pomyslně stíral rozdíly v historii vývoje ochrany osobních údajů v zemích západní Evropy a České republiky. Tento zákon lze chápat jako živý dokument, který prostřednictvím novelizací zohledňoval evropské trendy a neustálý vývoj technologií.

3.2 Předpisy Evropského práva v oblasti ochrany a zpracování osobních údajů

3.2.1 Úvod do problematiky

Dne 4. května 2016 byly v Ústředním věstníku Evropské unie zveřejněny hned tři dokumenty související s ochranou osobních údajů. Tento den lze bez nadsázky považovat za zásadní v oblasti ochrany osobních údajů, a to nejen v rámci České republiky, nýbrž v celoevropském kontextu. Konkrétně se jedná o tyto dokumenty:

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně údajů), (dále jen „Obecné nařízení 2016/679“)²⁴;
- Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými

²² *Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy. Viz § 11 zákona č. 40/1964 Sb., občanský zákoník.*

²³ Zkušenosti spojené se sledováním osob a činností tajné policie.

²⁴ V odborných textech či hovorů se lze setkat s anglickou zkratkou GDPR (General Data Protection Regulation).

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 (dále jen „Trestněprávní směrnice 2016/680“);

- Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti (dále jen „PNR směrnice 2016/681“).²⁵

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

Za základní ustanovení výše uvedené trojice právních aktů lze jednoznačně označit Obecné nařízení 2016/679 jakožto předpis navazující na Směrnici 95/46/ES. Jeho hlavním cílem bylo sjednocení dosavadní roztržičnosti v provádění ochrany osobních údajů v zemích Evropské unie²⁶ a hlavně vymýcení rostoucích rozdílů při zpracování osobních údajů v tomto společenství. Vytvoření individuálních právních rámců v jednotlivých členských státech způsobovalo řadu problémů při realizaci volného oběhu informací, zboží a služeb a značný vývojový pokrok v informačních technologiích a pokračující globalizace začaly upozorňovat na to, že téměř dvacet let stará směrnice již není schopná udržet jednotný rámec ochrany osobních údajů. Nastalá situace si žádala revizi celého právního rámce v evropském prostoru, ale na základě zkušeností se Směrnicí 95/46/ES byla snaha Evropské komise vyvarovat se „národní tvořivosti“ v pravidlech ochrany osobních údajů. Logickým vyústěním byl návrh nařízení Evropské unie, které „*nahrazuje vnitrostátní právní předpis a analogicky jej lze z pohledu jeho adresáta označit za obdobu zákona.*“²⁷ Obdobně jako Směrnice 95/46/ES, tak i Obecné nařízení 2016/679 bylo reakcí na vývoj společenství. Tato nová právní úprava vstoupila v platnost 25. května 2016 s dvouletým odkladem účinnosti neboli aplikovatelnosti. Evropskou komisí bylo apelováno, aby odklad účinnosti členské státy využily k analýzám dopadu Obecného nařízení 2016/679 a na přípravu provedení nezbytných úprav v dosavadní praxi zpracování osobních údajů.

²⁵ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 16 a 17.

²⁶ A dále Islandu, Norska a Lichtenštejska.

²⁷ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 16.

V porovnání s předchozí legislativou je Obecné nařízení 2016/679 přísnější v nárocích na zákonnost zpracování, na odpovědnost správce při zabezpečení osobních údajů a na posuzování vlivu zpracování v kontextu s právem a svobodou jednotlivců. I přesto, že povinnost správce přijmout vhodná organizační a technická opatření pro zabezpečení osobních údajů byla stanovena již v zákoně č. 101/2000 Sb., nová legislativa vyžaduje, aby opatření správce zohlednila rozsah, povahu, kontext a účely zpracování a aby byl správce schopen přijatá opatření dokumentovat a případně doložit kontrolnímu orgánu. Mezi další povinnosti správce nově patří systematické vyhodnocování pravděpodobnosti a závažnosti rizik, jež mohou ze zpracování osobních údajů vyplývat, a to převážně v důsledku využívání nových technologií.

Struktura Obecného nařízení 2016/679 jakožto nařízení Evropské unie se od zákona liší především rozdělením na dvě části. První část – Preambuli, tvoří tzv. recitály, které lze označit za důvodovou zprávu přijetí této právní úpravy, a část druhou tvoří vlastní text podobný zákonu.²⁸ Zmíněné části od sebe nelze striktně oddělovat, protože v některých případech je propojení recitálů společně s články stěžejní pro pochopení daného výkladu.²⁹ Zmiňovaná provázanost je přehledně uvedena v tabulce 2.

Tabulka 2 Propojení článků a recitálů Obecného nařízení 2016/679

Čl.	Recitál	Čl.	Recitál	Čl.	Recitál	Čl.	Recitál
1	1 – 13	22	71, 72	45	103 – 107	70	139
2	14 – 21	23	73	46	108 – 109	75	140
3	22 – 25	24	74 – 77, 83	47	110	77	141
4	26 – 37	25	78	49	111 – 116	78	143
5	39	26	79	51	117 – 119	79	145
6	40 – 50	27	80	52	118, 120	80	142
7	32, 33, 42, 43	28	81	53	121	81	144
8	38	30	13, 39, 82	55	122	82	146, 147
9	51 – 56	32	83, 74 – 77	56	124 – 128	83	148, 150, 151
11	57	33	75, 85, 87, 88	57	123, 132	84	149, 152
12	58, 59	34	75, 86 – 88	58	129	85	153
13	60 – 62	35	75, 84, 89 - 93	60	124 – 128, 130, 131	86	154
14	60 – 62	36	94 – 96	61	133	88	155
15	63, 64	37	97	62	134	89	156 – 163
16	65	38	97	63	135	90	164
17	65, 66	39	97	64	136	91	165
18	67	40	98, 99	66	137, 138	92	166 – 170
20	68	42	100	68	139	94	171
21	69, 70	44	101 – 102	69	139	95	173

Zdroj: zpracováno dle PIERSTONE. *The full service law firm for the new economy.*

²⁸ Pouze s tím rozdílem, že vlastní text Obecného nařízení 2016/679 není členěn na paragrafy, nýbrž na články.

²⁹ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 23.

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

Trestněprávní směrnice 2016/680 obsahuje zvláštní pravidla pro ochranu osobních údajů a volný pohyb osobních údajů v oblastech justiční a policejní spolupráce v trestních věcech. Zpracování osobních údajů dle této směrnice je možné pouze za účelem „*prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů.*“³⁰ Jsou-li osobní údaje zpracovány pro jiné účely, vychází se z ustanovení Obecného nařízení 2016/679. Shodně s Obecným nařízením 2016/679 Trestněprávní směrnice 2016/680 pracuje s určením pověřence pro ochranu osobních údajů, jehož prioritou bude dodržování povinností v oblasti ochrany osobních údajů.

Důležité je zmínit, že z Trestněprávní směrnice 2016/680 je vyřazeno zpracování osobních údajů prováděné při výkonu činností, které nespadají do oblasti působnosti práva Evropské unie³¹, a stejně tak zpracování osobních údajů prováděné orgány, institucemi a jinými subjekty Evropské unie.³²

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

PNR³³ směrnice 2016/681 byla připravována více než 6 let a jejím hlavním účelem je zajištění bezpečnosti, ochrany života a bezpečí osob a tvorba právního rámce pro ochranu údajů jmenné evidence cestujících „PNR“.³⁴

³⁰ *Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro ochranu osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují využívat osobní údaje v nebyvalém rozsahu pro účely provádění činností, jako jsou prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů. Viz recitál 3 trestněprávní směrnice 2016/680.*

³¹ Například činnosti týkající se národní bezpečnosti.

³² EPRAVO.CZ – Váš průvodce právem. *Další nařízení a směrnice z dílny Bruselu – tentokráte o ochraně osobních údajů* [online]. [cit. 2018-02-21]. Dostupné z WWW: <https://www.epravo.cz/top/clanky/dalsi-narizeni-a-smernice-z-dilny-bruselu-tentokrate-o-ochrane-osobnich-udaju-101840.html>.

³³ V anglickém originále „passenger names records“.

³⁴ Jmennou evidencí cestujících se rozumí evidence cestovních požadavků každého cestujícího, která obsahuje všechny potřebné informace, jež umožňují rezervujícím a zúčastněným leteckým dopravcům zpracovávat a kontrolovat rezervace u každé cesty rezervované kterýmkoliv cestujícím nebo jeho jménem bez ohledu na to, zda je uvedena v rezervačních systémech, kontrolních systémech odletů užívaných pro přihlášení cestujících k letu nebo jiných rovnocenných systémech poskytujících stejné funkce“.

PNR směrnice 2016/681 členskými státy nařizuje zřízení či určení orgánu příslušného pro prevenci, vyšetřování a stíhání teroristických činů a závažné trestné činnosti. Určený orgán je odpovědný za shromažďování údajů PNR od leteckých dopravců, jejich úschovu, zpracování, předání příslušným orgánům a výměnu těchto údajů s útvary pro informace o cestujících jiných členských států.³⁵

3.2.5 Shrnutí

Novou právní úpravu Evropské unie v souvislosti se zpracováním osobních údajů v čele s Obecným nařízením 2016/679 lze bez nadsázky chápat jako revoluční. Do současné doby totiž neexistoval právní předpis, který by upravoval tak rozsáhlý komplex vztahů. Tím, že Obecné nařízení 2016/679 zahrnuje i práva subjektů údajů, dá se hovořit o úpravě vztahů stovek milionů jedinců.

Luděk Nezmar ve své publikaci uvádí, že „nařízení GDPR je novátorské i v tom, že se netýká jen entit v rámci EU, ale kohokoliv, kdo chce zpracovávat data občanů EU. Firma z Hongkongu nebo nevládní organizace z USA působící na území Evropské unie tak musí vyhovět požadavkům GDPR stejně jako česká nebo slovenská firma.“³⁶

Kromě obecného nařízení mají zásluhu na zvýšení ochrany v oblasti osobních údajů také další nové směrnice Evropské unie, a to Trestně právní směrnice 2016/680 zaměřená na oblast ochrany fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonů trestů a tzv. PNR směrnice o používání údajů jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Tyto směrnice by v porovnání s Obecným nařízením 2016/679 neměly mít žádný dopad na správce či zpracovatele, jelikož jsou zaměřeny zejména na ochranu osobních údajů při činnosti orgánů činných v trestních řízeních.³⁷

Snad i vlivem silné medializace se nabytí účinnosti Obecného nařízení 2016/679 prvotně jevílo jako noční můra pro všechny správce a zpracovatele osobních údajů a v subjektech údajů vyvolávalo pocit narušující jejich svobodu, ale ve skutečnosti

³⁵ EPRAVO.CZ – Váš průvodce právem. *Další nařízení a směrnice z dílny Bruselu – tentokrát o ochraně osobních údajů* [online]. [cit. 2018-02-21]. Dostupné z WWW: <https://www.epravo.cz/top/clanky/dalsi-narizeni-a-smernice-z-dilny-bruselu-tentokrate-o-ochrane-osobnich-udaju-101840.html>

³⁶ NEZMAR, L. *GDPR: Praktický průvodce implementací*. 2017, s. 14.

³⁷ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 17.

je snahou evropského nařízení především snaha zabezpečit alespoň základní práva svobody běžného občana. V případě správců a zpracovatelů, kteří dosud respektovali ustanovení zákona č. 101/2000 Sb., bude implementace nové právní úpravy „*znamenat pouze vyjasnění postupů a jejich podřazení jednotlivým požadavkům vyplývajícím z Nařízení a korekce dosavadního zpracování.*“³⁸

3.3 Vývoj sankcí v právní úpravě ve veřejném právu

3.3.1 Sankce podle zákona č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Zákon č. 256/1992 Sb. byl prvním uceleným právním předpisem zabývajícím se ochranou osobních údajů v České a Slovenské Federativní Republice. Jedná se o právní předpis, jehož nedostatkem nebylo jen to, že řešil pouze zpracování v informačních systémech, ale že navíc nebyl postaven na klasické struktuře právní normy. Konkrétně v případě zákona č. 256/1992 Sb. chyběly sankce za jeho porušení a také zákon pozbýval ustanovení ohledně zřízení kontrolního orgánu.

I přesto, že v 90. letech 20. století zákon č. 256/1992 Sb. nezohledňoval sankce za možné porušení ochrany osobních údajů, bylo nutné tato případná porušení adekvátně řešit. V době charakteristické rozvojem technologií, počítačů a především internetu začalo ruku v ruce docházet k neoprávněnému nakládání s osobními údaji. Ochrana v této oblasti byla poskytována na základě § 178 zákona č. 140/1961 Sb., trestního zákona ve znění pozdějších předpisů (dále jen „trestní zákon“), který v případě neoprávněného nakládání s osobními údaji pachateli ukládal trest odnětí svobody v rozmezí 1 - 5 let, zákaz činnosti popř. peněžitý trest (viz tabulka 3).

Stejným právním předpisem jako v případě neoprávněného nakládání s osobními údaji byla řešena i trestněprávní ochrana na soukromí, a to konkrétně dle ustanovení § 206 trestního zákona (viz tabulka 4).

³⁸ JANEČKOVÁ, E. *GDPR. Praktická příručka implementace*. 2018, s. 119.

Tabulka 3 Postihy při neoprávněném nakládání s osobními údaji

Způsob neoprávněného nakládání s osobními údaji	Postih dle trestního zákona
Kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si присvojí osobní údaje o jiném shromážděné v průběhu trestního řízení nebo v souvislosti s výkonem veřejné správy a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. ³⁹	Odnětí svobody až na 3 roky nebo zákaz činnosti nebo peněžitý trest
Kdo, byť i z nedbalosti, poruší právním předpisem stanovenou povinnost mlčenlivosti tím, že sdělí nebo zpřístupní osobní údaje o jiném získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. ⁴⁰	
Kdo spáchá jeden či druhý výše uvedený čin tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem, nebo spáchá-li tento čin porušením povinností vyplývajících z jeho povolání, zaměstnání nebo funkce. ⁴¹	Odnětí svobody na 1 až 5 let nebo zákaz činnosti nebo peněžitý trest

Zdroj: zpracováno dle § 178 trestního zákona.

Tabulka 4 Postihy za šíření pomluvy

Pomluva	Postih dle trestního zákona
Kdo o jiném sdělí nepravdivý údaj, který je způsobitelný značnou měrou ohrozit jeho vážnost u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu. ⁴²	Odnětí svobody až na 1 rok
Kdo spáchá výše uvedený čin tiskem, filmem, rozhlasem, televizí nebo jiným obdobně účinným způsobem. ⁴³	Odnětím svobody až na 2 roky nebo zákazem činnosti

Zdroj: zpracováno dle § 206 trestního zákona.

V souvislosti s absencí kontrolního orgánu se v následujícím roce objevila snaha o jeho zřízení, ale návrh bohužel nebyl uveden do praxe a v budoucnu se k němu již nikdo nevrátil. Výše uvedený nedostatek zákona „nahrával“ především podnikatelům, kteří bez zábran získávali údaje o adresátech pro své reklamy a o potenciálních zákaznících. Data byla čím dál častěji zneužívána, jednotlivci obtěžováni a docházelo k nárůstu trestné činnosti.

³⁹ § 178 odst. 1 trestního zákona.

⁴⁰ § 178 odst. 2 trestního zákona.

⁴¹ § 178 odst. 3 trestního zákona.

⁴² § 206 odst. 1 trestního zákona.

⁴³ § 206 odst. 2 trestního zákona.

3.3.2 Sankce podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Ke zlepšení situace na poli ochrany osobních údajů dochází až nabytím účinnosti zákona č. 101/2000 Sb. Tento právní předpis nahradil původní zákon č. 256/1992 Sb. a doplnil jeho zásadní nedostatky. Zavedl sankce za porušení povinností stanovených zákonem a zřídil ÚOOÚ jako dozorový úřad nad dodržováním povinností stanovených při zpracování osobních údajů.⁴⁴ Horní hranici sankce za spáchání přestupku fyzických osob stanovuje na 5 000 000 Kč (blíže viz tabulka 5).

Tabulka 5 Sankce za přestupky fyzických osob

Přestupky - fyzické osoby
Možnost uložení pokuty do výše 100 000 Kč
Porušení mlčenlivosti fyzické osoby, která: a) je ke správci nebo zpracovateli v pracovním nebo jiném obdobném poměru, b) vykonává pro správce nebo zpracovatele činnosti na základě dohody, nebo c) v rámci plnění zvláštním zákonem uložených oprávnění a povinností přichází u správce nebo zpracovatele do styku s osobními údaji.
Možnost uložení pokuty do výše 1 000 000 Kč
Fyzická osoba jako správce nebo zpracovatel se dopustí přestupku tím, že při zpracování osobních údajů: a) nestanoví účel, prostředky nebo způsob zpracování nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona, b) zpracovává nepřesné osobní údaje, c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu, d) uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování, e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně, f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem, g) odmítne subjektu údajů poskytnout požadované informace, h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů, i) nesplní oznamovací povinnost podle tohoto zákona, nebo j) neprovede ve stanovené lhůtě uložené opatření k nápravě.
Fyzická osoba se dopustí přestupku tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem.

⁴⁴ (1) Zřizuje se Úřad pro ochranu osobních údajů se sídlem v Praze (dále jen „Úřad“).

(2) Úřad je ústředním správním úřadem pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem, zvláštními právními předpisy, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropské unie.

(3) Úřad vykonává působnost dozorového úřadu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu. Viz § 2 zákona č. 101/2000 Sb.

Možnost uložení pokuty do výše 5 000 000 Kč
<p>Fyzická osoba jako správce nebo zpracovatel se dopustí přestupku tím, že při zpracování osobních údajů některým z výše uvedených způsobů:</p> <p>a) ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo</p> <p>b) poruší povinnosti pro zpracování citlivých údajů.</p> <p>Fyzická osoba se dopustí přestupku tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem, a to prostřednictvím tisku, filmu, rozhlasu, televize, veřejně přístupné počítačové sítě nebo jiným obdobně účinným způsobem.</p>

Zdroj: zpracováno dle § 44 a 44a zákona č. 101/2000 Sb., o ochraně osobních údajů.

V případě správních deliktů způsobených právními osobami je horní hranice pokuty posunuta až na výši 10 000 000 Kč (viz tabulka 6).

Tabulka 6 Sankce za správní delikty právnických osob

Správní delikty - právní osoby
Možnost uložení pokuty do výše 1 000 000 Kč
Právní osoba nebo podnikající fyzická osoba se dopustí správního deliktu tím, že poruší zákaz zveřejnění osobních údajů stanovený jiným právním předpisem.
Možnost uložení pokuty do výše 5 000 000 Kč
<p>Právní osoba nebo fyzická osoba podnikající podle zvláštních předpisů se jako správce nebo zpracovatel dopustí správního deliktu tím, že při zpracování osobních údajů:</p> <p>a) nestanoví účel, prostředky nebo způsob zpracování, nebo stanoveným účelem zpracování poruší povinnost nebo překročí oprávnění vyplývající ze zvláštního zákona,</p> <p>b) zpracovává nepřesné osobní údaje,</p> <p>c) shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu,</p> <p>d) uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování,</p> <p>e) zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně,</p> <p>f) neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem,</p> <p>g) odmítne subjektu údajů poskytnout požadované informace,</p> <p>h) nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů,</p> <p>i) nesplní oznamovací povinnost podle tohoto zákona,</p> <p>j) nevede přehled případů porušení ochrany osobních údajů podle § 88 odst. 7 zákona o elektronických komunikacích,⁴⁵ nebo</p> <p>k) neprovede ve stanovené lhůtě uložené opatření k nápravě.</p> <p>Právní osoba nebo podnikající fyzická osoba se dopustí správního deliktu tím, že poruší zákaz</p>

⁴⁵ Podnikatel poskytující veřejně dostupnou službu elektronických komunikací vede pouze pro účely přezkumu plnění povinností podle odstavců 4 a 5 přehled porušení ochrany osobních údajů, včetně informací o okolnostech porušení, jeho dopadech a opatření přijatých k nápravě stavu. Prováděcí právní předpis může stanovit podrobnější podmínky, za nichž je podnikatel poskytující veřejně dostupnou službu elektronických komunikací povinen oznámit porušení ochrany osobních údajů, formát tohoto oznámení a způsob, jakým se má oznámení učinit. Viz § 88 odst. 7 zákona č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

zveřejnění osobních údajů stanovený jiným právním předpisem, a to prostřednictvím tisku, filmu, rozhlasu, televize, veřejně přístupné počítačové sítě nebo jiným obdobně účinným způsobem.
Možnost uložení pokuty do výše 10 000 000 Kč
Právník osoba jako správce nebo zpracovatel se dopustí správního deliktu tím, že při zpracování osobních údajů některým z výše uvedených způsobů: a) ohrozí větší počet osob svým neoprávněným zasahováním do soukromého a osobního života, nebo b) poruší povinnosti pro zpracování citlivých údajů.

Zdroj: zpracováno dle § 45 a 45a zákona č. 101/2000 Sb.

3.3.3 Sankce podle zákona č. 110/2019 Sb., o zpracování osobních údajů

V souvislosti s nabytím účinnosti Obecného nařízení 2016/679 byla jednou z nejobávanějších oblastí právě výše pokut, které nařízení v případě jeho porušení umožňuje udělit. Dle možného dopadu porušení zájmu chráněného tímto nařízením jsou druhy porušení rozděleny do dvou kategorií. Jak blíže uvádí Jiří Žůrek: „*Porušení povinnosti, jejíž nedodržení více ohrožuje zájem chráněný Obecným nařízením, spadá do kategorie s možnou vyšší sankcí než nedodržení povinnosti, které chráněný zájem ohrožuje méně.*“⁴⁶ Pro lepší pochopení zmiňovaných kategorií obsahují následující tabulky přehled nejčastějších porušení, ke kterým může především u správce⁴⁷ v praxi dojít.

Tabulka 7 Porušení povinností odpovídající pokutě do výše 10 000 000 EUR

Pokuta do výše 10 000 000 EUR nebo, jde-li o podnik, až do výše 2 % celkového ročního obrátu
Za porušení:
povinností při zabezpečení ochrany osobních údajů
podmínek pro najmutí a spolupráci se zpracovatelem
povinnosti vyhotovit záznamy o činnostech zpracování
povinnosti spolupráce s dozorovým úřadem
povinností při ohlašování případu porušení zabezpečení osobních údajů dozorovému úřadu, resp. subjektu údajů
povinnosti posoudit vliv na ochranu osobních údajů a absolvovat předchozí konzultaci
povinností týkajících se jmenování a podmínek pověřence
povinnosti ustanovit zástupce pro správce nebo zpracovatele usídleného mimo EU
povinnosti týkající se činnosti při získávání osvědčení

Zdroj: zpracováno dle ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 183.

⁴⁶ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 181. Např. více ohrožovat práva a svobody subjektů údajů bude nedodržení zásad zpracování osobních údajů než nedodržení povinnosti zpracovávat záznamy o činnostech zpracování.

⁴⁷ A tam, kde přichází v úvahu i zpracovatel.

V porovnání s předchozími případy následující tabulka obsahuje závažnější případy porušení Obecného nařízení 2016/679 a s tím ruku v ruce spojně i vyšší sankce.

Tabulka 8 Porušení povinností odpovídající pokutě do výše 20 000 000 EUR

Pokuta do výše 20 000 000 EUR nebo, jde-li o podnik, až do výše 4 % celkového ročního obrátu
Za porušení:
zásad a zákonnosti zpracování
podmínek vyjádření souhlasu
podmínek pro zpracování zvláštních kategorií osobních údajů
práv subjektu údajů
povinnosti vyplývající z právních předpisů členského státu, která se týká zvláštních situací, při nichž dochází ke zpracování, které Obecné nařízení umožňuje na vnitrostátní úrovni
povinnosti splnit příkaz nebo dočasné či trvalé omezení zpracování nebo přerušování toků údajů dozorovým úřadem ⁴⁸ nebo neposkytnutí přístupu ⁴⁹
nesplnění příkazu dozorového úřadu podle čl. 58 odst. 2 (nápravné pravomoci) nebo neposkytnutí přístupu při uplatnění dozorové pravomoci

Zdroj: zpracováno dle ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 184.

Česká republika v oblasti sankcí využila výjimek, které jsou členským státům umožněny, na základě čehož v zákoně č. 110/2019 Sb., o zpracování osobních údajů (dále jen “zákon č. 110/2019 Sb.”) zůstávají pro fyzické osoby jakožto správce či zpracovatele sankce stejné jako v zákoně č. 101/2000 Sb., a to do maximální výše 5 000 000 Kč, pro právnické osoby pak do výše 10 000 000 Kč (viz tabulky 5 a 6, kapitola 3.3.2). I přes ustanovení zákona o horních hranicích pokut české právo vylučuje, aby pokuty byly likvidační. Jak ukazuje dosavadní praxe, například nejvyšší pokuta uložená obci odpovídá hodnotě 80 000 Kč.⁵⁰

Zcela specifickou oblast představuje ukládání správních pokut orgánům veřejné moci a veřejným subjektům. Jelikož Obecné nařízení 2016/679 umožňuje členským státům stanovit podrobnější pravidla, český zákonodárce toho využil a v § 62 odst. 5 zákona č. 110/2019 Sb. stanovuje, že ÚOOÚ upustí od uložení správního trestu, jedná-li se o správce a zpracovatele zahrnuté v čl. 83 odst. 7 Obecného nařízení 2016/679.⁵¹ Žůrek

⁴⁸ V souladu s čl. 58 odst. 2 Obecného nařízení 2016/679.

⁴⁹ V souladu s čl. 58 odst. 1 písm. f) Obecného nařízení 2016/679.

⁵⁰ Právní rozhledy: časopis pro všechna právní odvětví. *Vláda schválila návrh zákona o zpracování osobních údajů*. 8/2018.

⁵¹ *Aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě. Viz. čl. 83 odst. 7 Obecného nařízení 2016/679.*

dodává „dá se tedy konstatovat, že orgány veřejné moci a veřejné subjekty jsou zproštěny možnosti udělit jim pokutu ze strany Úřadu pro ochranu osobních údajů, pokud nebudou dodržovat GDPR.“⁵²

Z výše uvedeného vyplývá, že ÚOOÚ bude nucen v případě porušování Obecného nařízení 2016/679 vůči těmto subjektům využít jiná nápravná opatření, a to dle ustanovení v čl. 58 odst. 2 tohoto nařízení.⁵³

3.3.4 Shrnutí

Při nakládání s osobními údaji, které není v souladu se zákonem, se mohou fyzické či právnické osoby dopustit přestupku nebo trestného činu. Jelikož při přestoupení zákona dochází k porušení práva na ochranu osobnosti člověka, jenž chrání důležité atributy lidské existence (např. čest, soukromí, důstojnost apod.), jsou sankce stanoveny poměrně přísně. Jak již bylo zmíněno výše, zákon č. 256/1992 Sb. sankce stanovit opomněl, ale následující zákon postihy za porušování povinností při nakládání s osobními údaji stanovil již dostatečně. Přijetím zákona č. 101/2000 Sb. došlo k zásadnímu posílení práv subjektů údajů a k požadovanému zaručení ochrany minimalizující neoprávněné zásahy do jejich soukromí.

Obecné nařízení 2016/679 nově zavádí horní hranici sankcí za jeho porušení až do výše 20 000 000 EUR, resp. 4% celkového ročního obratu, což se na první pohled může zdát jako částka likvidační, ale vezmeme-li v potaz roční obraty některých světových

⁵² ŽŮREK, J. *GDPR v personalistice*. 2019, s. 171.

⁵³ Každý dozorový úřad má všechny tyto nápravné pravomoci:

- a) upozornit správce či zpracovatele, že zamýšlené operace zpracování pravděpodobně porušují toto nařízení;
 - b) udělit napomenutí správci či zpracovateli, jehož operace zpracování porušily toto nařízení;
 - c) nařídit správci nebo zpracovateli, aby vyhověli žádostem subjektu údajů o výkon jeho práv podle tohoto nařízení;
 - d) nařídit správci či zpracovateli, aby uvedl operace zpracování do souladu s tímto nařízením, a to případně předepsaným způsobem a ve stanovené lhůtě;
 - e) nařídit správci, aby subjektu údajů oznámil případy porušení zabezpečení osobních údajů;
 - f) uložit dočasné nebo trvalé omezení zpracování, včetně jeho zákazu;
 - g) nařídit opravu či výmaz osobních údajů nebo omezení zpracování podle článků 16, 17 a 18 a ohlašování takových opatření příjemcům, jimž byly osobní údaje zpřístupněny podle čl. 17 odst. 2 a článku 19;
 - h) odebrat osvědčení nebo nařídit, aby subjekt pro vydávání osvědčení odebral osvědčení vydané podle článků 42 a 43, nebo aby osvědčení nevydal, pokud požadavky na osvědčení plněny nejsou nebo již přestaly být plněny;
 - i) uložit správní pokutu podle článku 83 vedle či namísto opatření uvedených v tomto odstavci, podle okolností každého jednotlivého případu;
 - j) nařídit přerušování toků údajů příjemci ve třetí zemi nebo toků údajů mezinárodní organizaci.
- Viz čl. 58 odst. 2 Obecného nařízení 2016/679.

společností typu Google⁵⁴, je stanovená částka zcela adekvátní. Pokud je snahou Evropské unie odradit tyto společnosti od dalšího neoprávněného zpracování osobních údajů, stanovené výše pokut tento jejich zámysl rozhodně podporují.

Česká republika, zřejmě na základě zkušeností z předchozích let, ponechává v zákoně č. 110/2019 Sb. horní hranice pokut ve výši stanovené již zákonem č. 101/2000 Sb. I přes počáteční obavy z navýšení správních pokut vláda v České republice vyhodnotila stávající částky jako účinné, přiměřené a zároveň odrazující.⁵⁵

Zcela odchylná pravidla pro ukládání správních pokud jsou stanovena pro orgány veřejné moci a veřejné subjekty, kdy zákon č. 110/2019 Sb. umožňuje Úřadu pro ochranu osobních údajů upustit od uložení správního trestu a dle evropského právního aktu využít jiné nápravné pravomoci.

3.4 Srovnání zákona č. 101/2000 Sb., o ochraně osobních údajů se zákonem č. 110/2019 Sb., o zpracování osobních údajů se zaměřením na nový přístup k osobním údajům

3.4.1 Nové přístupy

Obecné nařízení 2016/679 nabylo účinnosti dnem 25. května 2018, čímž se stalo přímo závazným ve všech zemích Evropské unie. Jelikož stanovuje práva a povinnosti při zpracování osobních údajů, nahrazuje v tomto rozsahu zákon č. 101/2000 Sb. Původně mělo dojít pouze k jeho novelizaci, ale nakonec bylo odsouhlaseno zrušení a navrzení zcela nového právního předpisu. Účinnost zákona o ochraně osobních údajů skončila dnem 12. března 2019, kdy došlo k nabytí účinnosti zákona č. 110/2019 Sb., o zpracování osobních údajů.

Zákon č. 110/2019 Sb. reaguje v první řadě na přijetí Obecného nařízení 2016/679, ale promítá se do něj i implementace Trestněprávní směrnice 2016/680. Jeho snahou není

⁵⁴ Google, Inc. - americká akciová společnost vlastněná holdingovou společností Alphabet Inc, založená 4. 9. 1998. Internetový vyhledávač Google je v dnešní době nejpoužívanějším světovým internetovým vyhledávačem. Dle dostupných informací společnost vykazovala v roce 2016 roční obrát ve výši 94, 76 miliard USD.

⁵⁵ *Nejsou-li správní sankce harmonizovány tímto nařízením nebo v případě potřeby v jiných případech, jako jsou závažná porušení tohoto nařízení, měly by členské státy zavést systém, který zajistí uložení účinných, přiměřených a odrazujících pokut. Povaha těchto trestních nebo správních sankcí by měla být stanovena právem členského státu. Viz recitál 152 Obecného nařízení 2016/679.*

duplikace jednotlivých článků Obecného nařízení 2016/679, nýbrž úprava těch oblastí, ve kterých dostaly členské státy vlastní prostor pro volbu vhodné právní úpravy.⁵⁶

3.4.1.1 Teoretická východiska

K novému právnímu rámci ochrany osobních údajů došlo z toho důvodu, že stav původní, založený na Směrnici 95/46/ES, již přestal odpovídat současné době. Rozdíl lze spatřit zejména v pokrokových prostředcích využívaných ke zpracování osobních údajů, v komplexnějším zpracování dat a hlavně v prohlubujících se rozdílech v právní úpravě jednotlivých členských států Evropské unie.

V dnešním digitálním světě je málo pravděpodobné, že někdo odcizí kartotéku zaměstnanců či klientů v papírové podobě, naopak stále větší riziko vzniká u odcizení digitálních záznamů, kdy se může jednat o zcizení dat několikanásobného rozsahu.⁵⁷

3.4.1.2 Posun v novém zákoně o zpracování osobních údajů

Zákon č. 110/2019 Sb., o zpracování osobních údajů nabyl účinnosti dne 12. března 2019 a jeho hlavním cílem je zajištění souladu vnitrostátní právní úpravy s Obecným nařízením 2016/679, neboť nesplnění závazků plynoucích z členství v Evropské unii by v důsledku mohlo vést k uvalení finančních sankcí ze strany EU.⁵⁸

Sjednocená úroveň ochrany dat v celé Evropské unii zamezí rozdílům, které brání volnému pohybu osobních údajů v rámci vnitřního trhu a zabezpečí všem subjektům právní jistotu a transparentnost. Subjektům údajů bude ve všech členských státech zajištěna stejná úroveň práv vymahatelných stejnými právními prostředky, správci a zpracovatelé budou mít stejné povinnosti a popřípadě i rovnocenné sankce ve všech členských státech.

Zákon o zpracování osobních údajů nejde nad rámec úprav evropského nařízení, ale převážně zpřesňuje ty instituty, kde byla členskými státy poskytnuta možnost vlastního uvážení právní úpravy.

⁵⁶ EPRAVO.CZ – Váš průvodce právem. *Nový návrh zákona o zpracování osobních údajů: česká adaptace GDPR a dvojitá metr při ukládání pokut?* [online]. [cit. 2018-02-22]. Dostupný z: <https://www.epravo.cz/top/clanky/novy-navrh-zakona-o-zpracovani-osobnich-udaju-ceska-adaptace-gdpr-a-dvoji-metr-pri-ukladani-pokut-106385.html>

⁵⁷ BULLA, M. *Osobní údaje v elektronické podobě a GDPR*. In PaM 5/2018.

⁵⁸ EPRAVO.CZ – Váš průvodce právem. *Nový návrh zákona o zpracování osobních údajů: česká adaptace GDPR a dvojitá metr při ukládání pokut?* [online]. [cit. 2018-02-22]. Dostupný z: <https://www.epravo.cz/top/clanky/novy-navrh-zakona-o-zpracovani-osobnich-udaju-ceska-adaptace-gdpr-a-dvoji-metr-pri-ukladani-pokut-106385.html>

3.4.1.3 Volba orgánu příslušného k akreditaci certifikačních těles

Novou problematikou, kterou zákon č. 110/2019 Sb. musel zohlednit, je volba subjektů pro vydávání osvědčení. Oproti ustanovení zákona č. 101/2000 Sb. zavádí Obecné nařízení 2016/679 pro subjekty zpracující osobní údaje možnost získat osvědčení pro účely prokázání souladu s evropským nařízením. Z tohoto důvodu nařízení stanovuje, aby členské státy zajistily řádnou akreditaci subjektů pro vydávání osvědčení.⁵⁹

Zákon č. 110/2019 Sb. v § 15 stanovuje, že „*osoby oprávněné k vydávání osvědčení o ochraně osobních údajů jsou akreditovány osobou pověřenou k výkonu působnosti akreditačního orgánu podle zákona upravujícího akreditaci subjektů posuzování shody.*“⁶⁰

V České republice je jediným akreditačním orgánem pro certifikace splnění požadavků různých známek či certifikátů ochrany soukromí Český institut pro akreditaci, o.p.s.⁶¹

3.4.1.4 Ustavení nezávislého dozorového orgánu, zajištění jeho činnosti, procedura jmenování jeho vedení, zajištění nezávislosti vedení i zaměstnanců

V zákoně o zpracování osobních údajů je totožně jako v ustanovení zákona č. 101/2000 Sb. zřizován ÚOOÚ jakožto ústřední správní úřad, ale k podstatné změně dochází v upřesnění zajištění jeho činnosti⁶² či struktury. Paragraf 54 zákona o zpracování osobních údajů obsahuje rozšířený výčet povinností ÚOOÚ jak ve vztahu ke zpracování

⁵⁹ Aniž jsou dotčeny úkoly a pravomoci příslušného dozorového úřadu podle článků 57 a 58, osvědčení vydává a obnovuje subjekt pro vydávání osvědčení, který má příslušnou úroveň odborných znalostí ohledně ochrany údajů, a to poté, co informoval dozorový úřad s cílem umožnit případně výkon jeho pravomocí podle čl. 58 odst. 2 písm. h). Členské státy zajistí, aby byly tyto subjekty pro vydávání osvědčení akreditovány jedním nebo oběma z následujících orgánů:

a) dozorovým úřadem, který je příslušný podle článku 55 nebo 56; nebo

b) vnitrostátním akreditačním orgánem. Viz čl. 43 odst. 1 Obecného nařízení 2016/679.

⁶⁰ Viz § 15 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Zákonem upravujícím akreditaci subjektů posuzování shody se rozumí zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.

⁶¹ Český institut pro akreditaci, obecně prospěšná společnost, jako Národní akreditační orgán založený vládou České republiky poskytuje své služby v souladu s platnými právními předpisy ve všech oblastech akreditace jak státním, tak privátním subjektům. Princip jednotného evropského akreditačního systému tvořeného národními akreditačními orgány, které fungují podle jednotných pravidel a akreditují podle definovaných mezinárodně uznávaných norem, vychází z postoje ES specifikované v Globální koncepci o přístupu ke zkoušení a certifikaci.

⁶² § 54 zákona č. 110/2019 Sb., o zpracování osobních údajů.

osobních údajů dle hlavy II⁶³, tak ve vztahu ke zpracování osobních údajů, nejde-li o zpracování prováděné soudy a státními zastupitelstvy dle hlavy III.⁶⁴

Oproti ustanovení zákona č. 101/2000 Sb. zákon o zpracování osobních údajů již nepočítá s funkcí inspektorů, ale nově tvoří strukturu ÚOOÚ pouze předseda a dva místopředsedové. Předseda ÚOOÚ se zároveň stává členem Evropského sboru pro ochranu osobních údajů, nově vzniklého nezávislého dozorového úřadu, který bude mít mimo jiné i rozhodovací pravomoc. *„Tato činnost bude vysoce kvalifikovaná, odpovědná a úkoly budou muset být plněny v krátkých lhůtách.“*⁶⁵

Předseda ÚOOÚ má nově, dle § 52 odst. 1 zákona č. 110/2019 Sb., pravomoc pověřit místopředsedu trvalým plněním některých svých úkolů. Dále je ošetřena i zastupitelnost předsedy ÚOOÚ v době jeho nepřítomnosti. Jak uvádí § 53 odst. 2 zákona o zpracování osobních údajů, předsedu zastupuje ten funkcionář, který byl Senátem jmenován dříve, a to včetně zohlednění případného bezprostředně předcházejícího funkčního období.

Zákon č. 110/2019 Sb. zohledňuje i oblast nezávislosti ÚOOÚ, kdy v § 51 odst. 1 stanovuje, že *„při výkonu své působnosti v oblasti ochrany osobních údajů Úřad postupuje nezávisle a řídí se pouze právními předpisy a přímo použitelnými předpisy Evropské unie.“*⁶⁶

3.4.1.5 Případné doplňující sankce za porušení ochrany osobních údajů (kromě dosud existujících)

Součástí každé právní normy zpravidla bývá i sankční oblast, která má mít preventivní a donucovací účinky vůči adresátům této právní normy. Zákon o zpracování osobních údajů není výjimkou a rovněž upravuje problematiku týkající se postihů v případě porušení ochrany osobních údajů.

⁶³ Hlava II zákona č. 110/2019 Sb., o zpracování osobních údajů – Zpracování osobních údajů podle přímo použitelného předpisu Evropské unie.

⁶⁴ Hlava III zákona č. 110/2019 Sb., o zpracování osobních údajů – Ochrana osobních údajů při jejich zpracování za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti ČR nebo zajišťování veřejného pořádku a vnitřní bezpečnosti.

⁶⁵ GDPR, Obecné nařízení o ochraně osobních údajů prakticky. *Návrh nového zákona o ochraně osobních údajů je na světě* [online]. [cit. 2018-02-21]. Dostupný z: <https://www.gdpr.cz/blog/navrh-novely-zakona-c-1012000-sb-je-na-svete/>.

⁶⁶ *Do činnosti Úřadu lze zasahovat jen na základě zákona. Při výkonu své působnosti v oblasti ochrany osobních údajů Úřad postupuje nezávisle a řídí se pouze právními předpisy a přímo použitelnými předpisy Evropské unie.* Viz § 51 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Zákon č. 110/2019 Sb. nevyužívá možnosti zvýšit horní hranice sankcí dle možností uvedených v Obecném nařízení 2016/679⁶⁷, naopak je ponechává ve výši stanovené zákonem č. 101/2000 Sb. (blíže v kapitole 3.3.2 – Sankce podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů). Důvodem ponechání stávající výše pokut může být i fakt, že finanční prostředky pokutovaných institucí zpravidla plynou z veřejných rozpočtů. V důsledku by u právnických osob s menším rozpočtem v zásadě docházelo pouze k formálnímu přesunu finančních prostředků v rámci státního rozpočtu, neboť pokutované instituce by musely o finanční prostředky na úhradu sankcí dodatečně žádat.⁶⁸

3.4.1.6 Vyvážení svobody projevu a ochrany osobních údajů

V zákoně o zpracování osobních údajů nově dostává nemalý prostor také problematika spojená se zpracováním osobních údajů za účelem vědeckého nebo historického výzkumu či pro statistické účely a dále zpracování prováděné pro novinářské účely popřípadě pro účely akademického, uměleckého či literárního projevu. Větší zaměření na výše uvedenou oblast je určitě na místě, neboť kromě obav z výše pokut při porušení ochrany osobních údajů byla dalším obávaným strašákem svoboda slova a informací pro novináře a televizní stanice.

Na základě ustanovení čl. 85 Obecného nařízení 2016/679⁶⁹ upravuje zákon č. 110/2019 Sb. v § 16⁷⁰ a § 17⁷¹ základní pravidla zpracování osobních údajů pro výše

⁶⁷ Článek 83 odst. 4, 5 a 6 Obecného nařízení 2016/679.

⁶⁸ GDPR, Obecné nařízení o ochraně osobních údajů prakticky. *Návrh nového zákona o ochraně osobních údajů je na světě* [online]. [cit. 2018-02-21]. Dostupné z WWW: <https://www.gdpr.cz/blog/navrh-novely-zakona-c-1012000-sb-je-na-svete/>.

⁶⁹ Článek 85 Obecného nařízení 2016/679 – Zpracování a svoboda projevu a informací

1. Členské státy uvedou prostřednictvím právních předpisů právo na ochranu osobních údajů podle tohoto nařízení do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu.

2. Pro zpracování pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu členské státy stanoví odchylky a výjimky z kapitoly II (zásady), kapitoly III (práva subjektu údajů), kapitoly IV (správce a zpracovatel), kapitoly V (předávání osobních údajů do třetí země nebo mezinárodní organizaci), kapitoly VI (nezávislé dozorové úřady), kapitoly VII (spolupráce a jednotnost) a kapitoly IX (zvláštní situace, při nichž dochází ke zpracování osobních údajů), pokud je to nutné k uvedení práva na ochranu osobních údajů do souladu se svobodou projevu a informací.

3. Každý členský stát ohlásí Komisi právní ustanovení, která přijme podle odstavce 2, a bez prodlení jakékoliv následné novely nebo změny týkající se těchto ustanovení.

⁷⁰ § 16 zákona č. 110/2019 Sb., o zpracování osobních údajů – Zpracování osobních údajů za účelem vědeckého nebo historického výzkumu nebo pro statistické účely.

⁷¹ § 117 zákona č. 110/2019 Sb., o zpracování osobních údajů – Zpracování osobních údajů prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu.

uvedené účely. Snahou nového zákona je v mezích možností zachovat stávající stav a standard zvláště novinářské práce. Zákonná úprava by neměla prostor svobody tisku ani rozšiřovat, ani zužovat. V ideálním případě by v oblasti zpracování údajů pro novinářské účely, stejně tak pro účely akademického, uměleckého nebo literárního projevu, nemělo dojít k zásadním změnám oproti stávajícímu stavu.⁷²

3.4.2 Shrnutí

Dnem nabytí platnosti Obecného nařízení 2016/679 vyvstala České republice, stejně tak jako ostatním členům Evropské unie, povinnost adekvátním způsobem na situaci reagovat. Výstupem České republiky v tomto směru byl zákon č. 110/2019 Sb., o zpracování osobních údajů, jakožto právní předpis nahrazující zákon č. 101/2000 Sb., o ochraně osobních údajů. Hlavním cílem nového zákona a s tím spojenou novelizací právních předpisů je nejen implementace Obecného nařízení 2016/679, ale i Trestněprávní směrnice 2016/680, jakožto právního předpisu regulujícího „zpracování údajů v rámci policejní spolupráce a justiční spolupráci v trestních věcech.“⁷³

Za zásadní změny v nové právní úpravě lze považovat zcela nová či výslovně upravená práva subjektu údajů (právo „být zapomenut“ či právo na přenositelnost údajů), zavedení pověřence pro ochranu osobních údajů či upřesnění zajištění činnosti a struktury nezávislého dozorového orgánu.

Naopak minimálně byla Českou republikou využita možnost navýšit sankce v případě porušení povinností či zpřísnění podmínek při zpracování osobních údajů pro novinářské účely nebo pro účely akademického, uměleckého či literárního projevu. V obou případech se spíše jednalo o snahu zachovat stávající stav.

⁷² GDPR, Obecné nařízení o ochraně osobních údajů prakticky. *Návrh nového zákona o ochraně osobních údajů je na světě* [online]. [cit. 2018-02-21]. Dostupný z: <https://www.gdpr.cz/blog/navrh-novely-zakona-c-1012000-sb-je-na-svete/>.

⁷³ I. Obecná část písm. A) odst. 3 Důvodové zprávy Zákona o zpracování osobních údajů.

4 Praktická část

4.1 Zaměření na konkrétní útvar AČR

4.1.1 Ozbrojené síly České republiky

Tato kapitola pojednává o ozbrojených silách ČR, jejich hlavních úkolech, postavení a struktuře. Blíže se na uvedenou problematiku zaměřuje zákon č. 219/1999 Sb., o ozbrojených silách České republiky ve znění pozdějších předpisů (dále jen „zákon o ozbrojených silách“). Jak stanovuje § 3 odst. 1 zákona o ozbrojených silách, Česká republika tyto síly vytváří především kvůli zajištění své bezpečnosti. Jejich hlavním úkolem je co nejefektivnější a nejlepší zabezpečení obrany území ČR s využitím zásad kolektivní obrany dle čl. 5 Washingtonské smlouvy NATO.⁷⁴

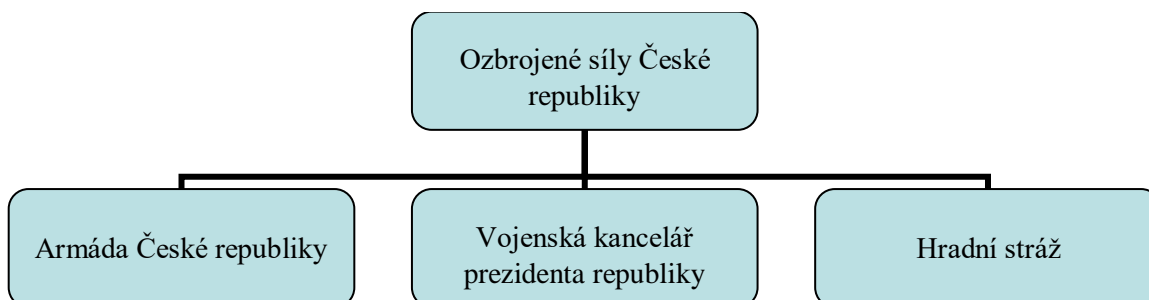
Ozbrojené síly tvoří:

- Armáda České republiky (dále jen „AČR“) – hlavní subjekt realizace obrany republiky. Zabezpečuje nepřetržitou, nezávislou a efektivní přípravu pro obranu českého národa před napadením nepřítele;
- Vojenská kancelář prezidenta republiky – zabezpečuje úkoly související s výkonem pravomocí prezidenta republiky jakožto vrchního velitele ozbrojených sil a dále řízení Hradní stráže;
- Hradní stráž – samostatná plně profesionální složka ozbrojených sil, která zajišťuje ostrahu a obranu Pražského hradu a dalších objektů a zabezpečuje organizaci vojenských poct při oficiálních příležitostech. Tvoří ji dva prapory, a to hudba Hradní stráže a rota zabezpečení.

⁷⁴ Washingtonská smlouva je zakládajícím a hlavním dokumentem Severoatlantické aliance, který při vstupu do Aliance podepisují a schvalují všechny členské země. Česká republika tak učinila v roce 1999.

Článek 5 Washingtonské smlouvy NATO - *Smluvní strany se dohodly, že ozbrojený útok proti jedné nebo více z nich v Evropě nebo Severní Americe bude považován za útok proti všem, a proto se dohodly, že dojde-li k takovému ozbrojenému útoku, každá z nich, uplatňujíc právo na individuální nebo kolektivní sebeobranu uznané článkem 51 Charty OSN, pomůže smluvní straně nebo stranám takto napadeným tím, že neprodleně podnikne sama a v součinnosti s ostatními stranami takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a zachovat bezpečnost severoatlantického prostoru. Každý takový útok a veškerá opatření učiněna v jeho důsledku budou neprodleně oznámena Radě bezpečnosti. Tato opatření budou ukončena, jakmile Rada bezpečnosti přijme opatření nutná pro obnovení a zachování mezinárodního míru a bezpečnosti.*

Obrázek 1 Struktura ozbrojených sil České republiky



Zdroj: vlastní zpracování

4.1.2 Armáda České republiky

Armáda České republiky, kterou lze chápat jako základ ozbrojených sil, je zapojena do integrované vojenské struktury NATO, do systému obranného, operačního a civilního nouzového plánování, do procedurálních a organizačních aspektů jaderných konzultací a do společných cvičení a operací.⁷⁵ Dále je zapojena do vojenské struktury EU a v součinnosti s tím se zúčastňuje společných cvičení a mezinárodních operací. V jejím čele stojí Generální štáb AČR, jehož náčelníkem je armádní generál Aleš Opata⁷⁶, přičemž jednotlivé druhy vojsk samostatně řídí velitelství pozemních a vzdušných sil.

Pozemní síly AČR slouží k vytváření a přípravě úkolových uskupení pozemních sil vyčleněných pro řešení taktických či operačně taktických úkolů na území ČR i mimo něj a dále k plnění dalších úkolů stanovených zákonem. Od 1. 6. 2018 je velitelem pozemních sil generálmajor Josef Kopecký.

Mezi hlavní úkoly pozemních sil patří vedení obranné a útočné bojové činnosti, ochrana komunikací, objektů a prostorů mimo oblast přímé bojové činnosti či sledování situace v přiděleném prostoru při mírových a zahraničních operacích. V případě potřeby příslušníci pozemních sil posilují ochranu státní hranice, střežení klíčových objektů na území ČR a v neposlední řadě plnění úkolů ve prospěch Policie ČR.⁷⁷

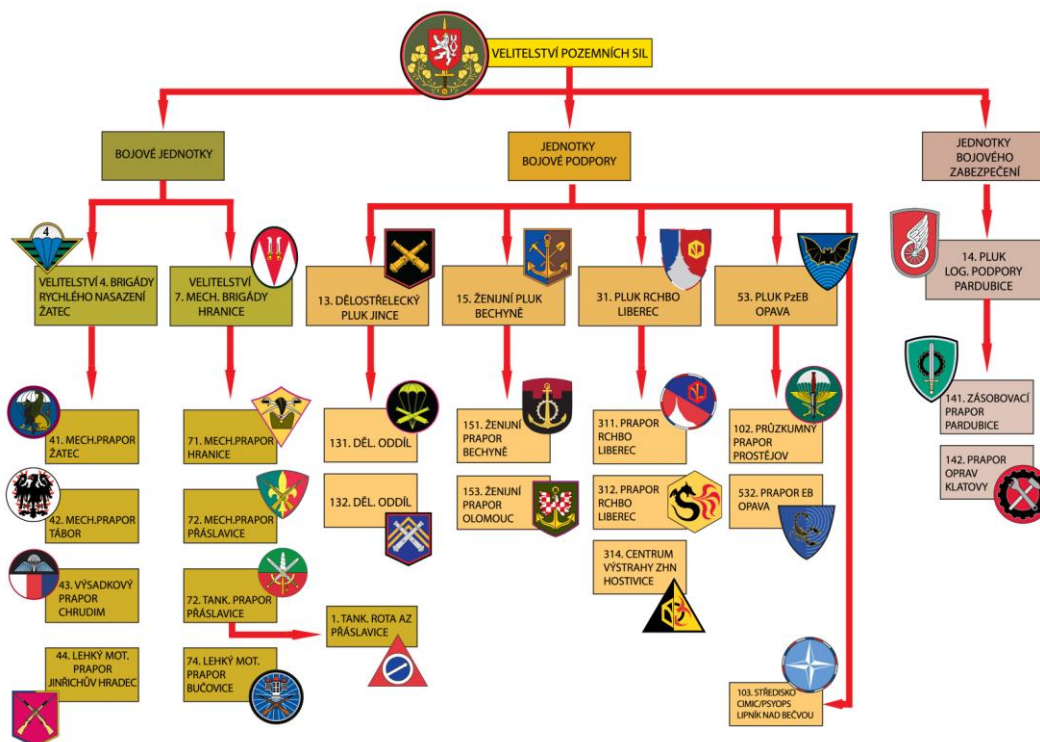
⁷⁵ ARMY.CZ, Armáda České republiky. *Armáda České republiky se představuje* [online]. [cit. 2018-07-11]. Dostupný z: <http://www.acr.army.cz/scripts/detail.php?id=5090>

⁷⁶ Armádní generál Aleš Opata byl do funkce jmenován dne 1. 5. 2018. Jeho předchůdcem byl armádní generál Josef Bečvář.

⁷⁷ ARMY.CZ, Armáda České republiky. *Struktura Velitelství pozemních sil AČR* [online]. [cit. 2018-07-11]. Dostupný z: <http://www.acr.army.cz/struktura/generalni-stab/velitelstvi-pozemnich-sil-86865/>

Pozemní síly AČR zahrnují bojové jednotky, jednotky bojové podpory a jednotky bojového zabezpečení, viz následující schéma.

Obrázek 2 Členění pozemních sil AČR



Zdroj: <http://www.acr.army.cz/vystroj/rukavove-znaky-vojaku-pozemnich-sil-acr-100034/>⁷⁸

Vzdušné síly AČR zabezpečují obranyschopnost, suverenitu a územní celistvost republiky a jejího vzdušného prostoru. Výše uvedené úkoly jsou plněny v rámci integrovaného systému protivzdušné a protiraketové obrany NATO. V případě ohrožení

⁷⁸ Vysvětlení zkratk z obrázku 2:

RCHBO - radiační, chemická a biologická ochrana.

ZHN – zbraně hromadného ničení.

PzEB - pluk průzkumu a elektronického boje. Elektronický boj je v současnosti definován jako vojenská činnost, zahrnující použití elektromagnetické a směrované energie s cílem ztížit nebo znemožnit využití elektromagnetického spektra protivníkem a řídit činnosti k zabezpečení efektivního využití elektromagnetického spektra vlastními silami.

CIMIC - koordinace činnosti a spolupráce mezi velitelem a představiteli státní správy a samosprávy, včetně místního obyvatelstva a také mezi mezinárodními, národními vládními i nevládními organizacemi a agenturami pro podporu mise. Spolupráce probíhá na úrovni vzájemné komunikace a pomoci nejen organizacím, ale i jednotlivcům.

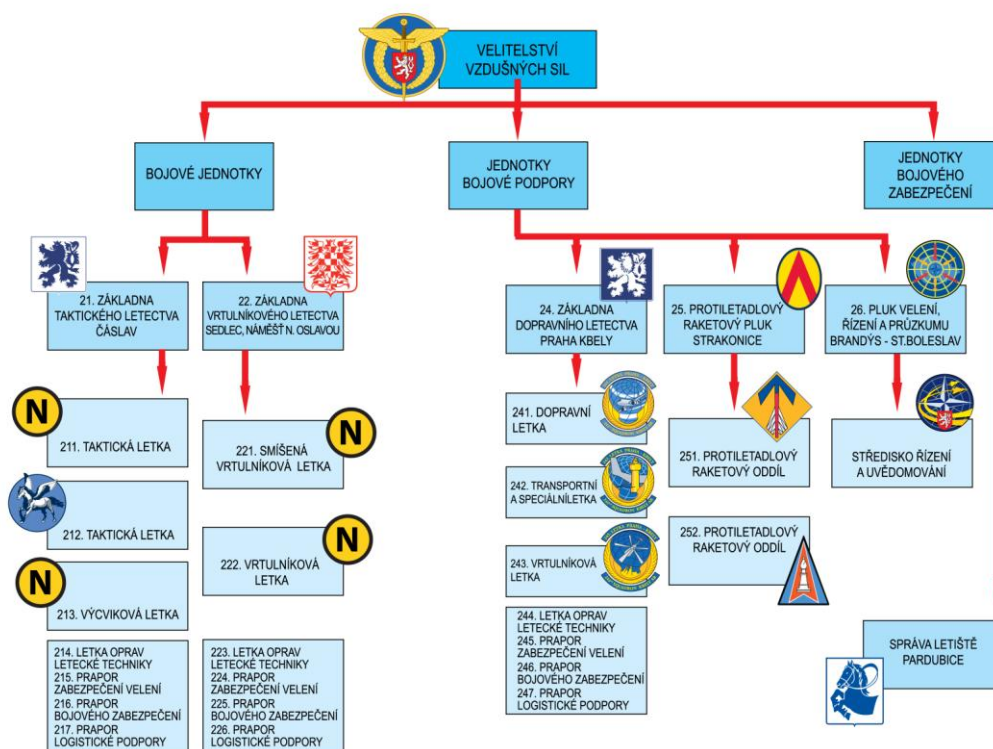
PSYOPS - plánované a cílevědomé psychologické působení na cílové skupiny, prováděné v době míru, za stavu vnějšího ohrožení státu a v době války, zaměřené na cílové skupiny k ovlivnění jejich postojů a chování, pro dosažení politických a vojenských cílů stanovených představiteli státu a AČR.

je systém podpořen aktivováním Národního posilového systému protivzdušné obrany.⁷⁹ Velitelem vzdušných sil byl dnem 1. 5. 2018 jmenován generálmajor Petr Hromek.

V mírovém životě vzdušné síly AČR zabezpečují pomoc posádkám letounů v nouzi, leteckou záchrannou službu ze stanoviště Plzeň – Líně či leteckou záchrannou službu ze stanoviště Plzeň – Líně. Dále se podílejí na přepravě ústavních a vládních činitelů a v případě živelných pohrom či katastrof jsou nápomocni Integrovanému záchrannému systému.⁸⁰

Podobně jako pozemní síly, tak i vzdušné jednotky jsou vázány k plnění aliančních závazků NATO a EU.⁸¹ Vzdušné síly AČR mají obdobnou strukturu jako pozemní síly, viz následující schéma.

Obrázek 3 Členění vzdušných sil AČR



Zdroj: <http://www.acr.army.cz/vystroj/rukavove-znaky-vojaku-vzdušnych-sil-acr-100033/>

⁷⁹ ARMY.CZ, Armáda České republiky. *Struktura Velitelství vzdušných sil AČR* [online]. [cit. 2018-07-11]. Dostupný z: <http://www.acr.army.cz/struktura/generalni-stab/velitelstvi-vzdušnych-sil-86864/>

⁸⁰ Tamtéž.

⁸¹ Zejména se jedná o přípravu jednotky vysoké připravenosti protiletadlového raketového vojska a poradního týmu vyčleněného pro výcvik příslušníků afghánského vrtulníkového letectva

4.1.3 41. mechanizovaný prapor v Žatci

Pro potřeby praktické části této diplomové práce byl vybrán jeden útvar ozbrojených sil AČR, konkrétně 41. mechanizovaný prapor v Žatci (dále jen „41. mpr“). Jedná se o útvar spadající pod bojové jednotky 4. brigády rychlého nasazení Velitelství pozemních sil AČR. Prapor byl vybrán z toho důvodu, že jsem již čtrnáctým rokem jeho součástí, v posledních několika letech na služebním místě Náčelník skupiny ochrany utajovaných informací a také v roli bezpečnostního manažera organizačního celku.

4.1.3.1 Historie vzniku útvaru

Historie útvaru sahá až k přelomu let 1869 a 1870, kdy ve Vysokém Mýtě vznikl pod názvem zeměbranecký prapor č. 30 a působil zde až do vypuknutí 1. světové války. Během válečných konfliktů byl nasazen na různých místech, ale vždy se vracel do původní posádky, kde setrval až do července roku 1939, kdy po likvidaci československé branné moci zanikl.

Ke znovuzřízení pluku, opět ve Vysokém Mýtě, došlo ihned po skončení 2. světové války. Během následujících let došlo k několika reorganizacím, změnám názvu a dislokací, přičemž konečné umístění bylo ve městě Benešov. Úplný rozchod s původními tradicemi však znamenalo jeho přejmenování na pluk „Květnového povstání českého lidu“ v roce 1975.⁸²

V průběhu novodobé historie existence útvaru došlo v roce 1991 k transformaci na mechanizovaný pluk a v létě 1994 vznikl 41. mpr, tak jak jej znám dnes. V dubnu 2004 došlo k přemístění praporu z Benešova do Žatce a dne 28. října 2005 byl útvaru propůjčen historický název „generála Josefa MALÉHO.“⁸³

⁸² ARMY.CZ, Armáda České republiky. *41. mechanizovaný prapor, historie a současnost* [online]. [cit. 2018-07-14]. Dostupný z: <http://www.41mpr.army.cz/historie-soucasnost>

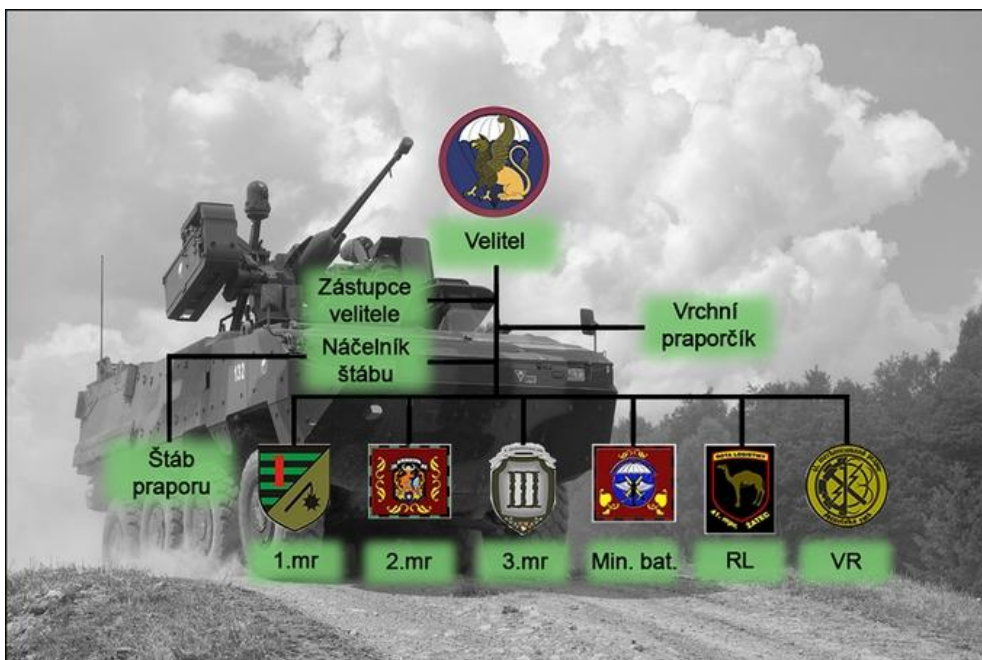
⁸³ Brigádní generál i. m. Josef MALÝ (nar. 3. 2. 1893) - český voják a člen ústředního vedení odbojové organizace Obrana národa, který byl pro svoji rozsáhlou a dlouhodobou odbojovou činnost koncem června 1941 zatčen gestapem a uvězněn ve věznici v Praze na Pankráci. Po nástupu nového zastupujícího říšského protektora Reinharda Heydricha byl společně s dalšími vysokými představiteli odboje odsouzen stanným soudem k trestu smrti a dne 1. 10. 1941 popraven v Praze – Ruzyni.

4.1.3.2 Současnost

41. mechanizovaný prapor „generála Josefa MALÉHO“ organizačně spadá do struktury 4. brigády rychlého nasazení⁸⁴, která je součástí Pozemních sil AČR. Útvar je vyčleněn především k plnění bojových a speciálních úkolů, a to nejen při bezprostředním ohrožení státu, ale i mimo území ČR. Ve zvláštních případech plní i úkoly nevojenského charakteru, např. při živelných pohromách.⁸⁵

Prapor disponuje nejnovější výzbrojí a výstrojí, které využívá z důvodu zachování vysokého stupně bojové připravenosti. Výcvik vychází z určení praporu a je závislý na výborné fyzické připravenosti všech příslušníků praporu bez ohledu na zařazení k bojovým či zabezpečovacím jednotkám (viz obrázek 4).

Obrázek 4 Struktura 41. mechanizovaného praporu



Zdroj: ARMY.CZ, Armáda České republiky. *41. mechanizovaný prapor, struktura* [online]. [cit. 2018-07-14]. Dostupný z: <http://www.41mpr.army.cz/struktura>

⁸⁴ 4. brigáda rychlého nasazení - „Obrany národa“ vznikla dne 1. 7. 1994, v současné době dislokována v Žatci.

⁸⁵ Například při likvidaci následků povodní v roce 2009 bylo v období 26. 6. – 29. 7. 2009 nasazeno 8 020 příslušníků AČR, odpracováno 80 200 hodin a nasazeno 2 047 kusů techniky.

4.1.3.3 Ochrana osobních údajů u 41. mpr před nabytím účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679

K naplnění povinnosti správce osobních údajů dle § 14 zákona č. 101/2000 Sb.⁸⁶ a dle čl. 13 RMO č. 16/2013 Věstníku O ochraně určených neutajovaných informací v rezortu Ministerstva obrany (dále jen „RMO č. 16/2013“) byla u 41. mpr před nabytím účinnosti Obecného nařízení 2016/679 zpracována Směrnice k zajištění ochrany osobních údajů (dále jen „Směrnice 41. mpr“), jakožto příloha Rozkazu velitele 41. mpr k zabezpečení organizovanosti chodu a života útvaru (dále jen „Organizační rozkaz“)⁸⁷. Směrnice 41. mpr stanovuje povinnosti zaměstnanců při zpracování osobních a citlivých údajů, konkrétně vymezuje účel a rozsah zpracovaných údajů, prostředky pro jejich zpracování, dobu uchování osobních údajů nezbytnou k naplnění stanoveného účelu a opatření k zajištění bezpečnosti údajů.

Kromě povinností zaměstnanců při zpracování osobních údajů Směrnice 41. mpr dále specifikuje problematiku označování těchto údajů, zvláštnosti při manipulaci s nimi či opatření z různých druhů bezpečnosti informací⁸⁸. K osobním údajům se ve Směrnici 41. mpr přistupuje stejně jako k určeným neutajovaným informacím⁸⁹, které jsou v čl. 3 odst. 2 písm. a) RMO č. 16/2013 definovány jako *„informace v jakékoli podobě, na jakémkoli nosiči, která byla vytvořena pouze pro vnitřní potřebu rezortu ministerstva nebo byla převzata od mimorezortních subjektů pro vnitřní potřebu rezortu ministerstva, jejíž neautorizované použití, modifikace, zničení nebo ztráta mohou způsobit narušení služebního zájmu, oprávněných zájmů osob nebo jinou škodu.“*⁹⁰

⁸⁶ Zaměstnanci správce nebo zpracovatele a jiné osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, mohou zpracovávat osobní údaje pouze za podmínek a v rozsahu správcem nebo zpracovatelem stanoveném.

⁸⁷ Základní dokument zřizovaný u každé vojenské součásti, který zohledňuje základní organizační záležitosti praporu, metodiky či postupy činností a to jak v pracovní, tak mimopracovní době. Dokument schvaluje vedoucí organizačního celku, s platností zpravidla na jeden kalendářní rok.

⁸⁸ Opatření administrativní, personální a fyzické a bezpečnosti.

⁸⁹ Správce k zajištění bezpečnosti osobních údajů aplikuje ustanovení hlavy II a V. Viz čl. 13 odst. 3 RMO č. 16/2013.

⁹⁰ Určenou neutajovanou informací se rozumí – informace v jakékoli podobě, na jakémkoli nosiči, která byla vytvořena pouze pro vnitřní potřebu rezortu ministerstva nebo byla převzata od mimorezortních subjektů pro vnitřní potřebu rezortu ministerstva, jejíž neautorizované použití, modifikace, zničení nebo ztráta mohou způsobit narušení služebního zájmu, oprávněných zájmů osob nebo jinou škodu a je informací, která není určena ke zveřejnění a nepodléhá zvláštní ochraně podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Viz čl. 3 odst. 2 písm. a) RMO č. 16/2013.

Problematika ochrany osobních údajů je dále řešena v již zmiňovaném Organizačním rozkaze, který v rámci nakládání s těmito údaji nařizuje:

- a) „provést seznámení určených zaměstnanců (včetně zastupujících zaměstnanců) s rozsahem jejich oprávnění a s podmínkami zpracování osobních údajů uvedenými ve Směrnici 41. mpr a stvrdit toto svým podpisem u Náčelníka skupiny ochrany utajovaných informací (dále jen „NSOUI“);
- b) předat neprodleně odpovědné osobě nový nebo aktualizovaný rozsah oprávnění a podmínek zpracování osobních údajů určených zaměstnanců v oblasti své působnosti v těchto případech: po reorganizaci, změně služebního zařazení zaměstnance, který zpracovává osobní údaje, nebo při vzniku nové evidence či agendy spojené se zpracováním osobních údajů;
- c) při změně služebního zařazení nebo v rámci jiné aktualizace doplnit personální skupinou u určených zaměstnanců oprávnění ke zpracování osobních údajů v jejich popisech pracovní činnosti.“⁹¹

V Organizačním rozkaze jsou dále v souvislosti s ochranou osobních údajů uvedena opatření k zamezení úniku osobních údajů v síti Internet a to v souladu se Standardním operačním postupem MO⁹². Důraz je kladen na dodržování pravidel v oblasti šíření či přenosu osobních údajů na sociálních sítích či prostřednictvím soukromých emailových adres. V souvislosti se zahraničními operacemi, poté na zveřejňování fotografií a osobních údajů vyslaných příslušníků AČR způsobem umožňujícím jejich ztotožnění a získání kontaktů jak na ně, tak na jejich rodinné příslušníky.

Vzhledem k charakteru útvaru a stále rostoucímu riziku možného zneužití osobních údajů má 41. mpr dále zpracován Plán zajištění kontinuity kritických činností v krizových nebo havarijních situacích (dále jen „Plán zajištění kontinuity“). Mimořádnou situaci lze definovat jako stav, kdy bezprostředně hrozí, že dojde k vyžrazení nebo zneužití osobních údajů. Plán zajištění kontinuity představuje souhrn obecných zásad řešení mimořádných situací popisujících činnost jednotlivých osob podílejících se na ochraně osobních údajů. Mezi modelové situace možného vyžrazení či zneužití osobních údajů považuje například neoprávněné nakládání s osobními údaji poučenými osobami, seznámení se s osobními

⁹¹ Viz Organizační rozkaz 41.mpr.

⁹² Standardní operační postup Ministerstva obrany č. 234 – Pravidla pro zveřejňování identity vojáků – Média. Blíže nelze specifikovat, určenou pouze PRO SLUŽEBNÍ POTŘEBU.

údaji nepovolanými osobami (např. při vloupání), zničení nebo poškození údajů živelnou pohromou či průmyslovou havárií⁹³. Stále aktuálnější jsou ovšem rizika spojena ne s nebezpečím pramenícím z přírodních živlů, ale spíše souvisejících s vlivem lidského faktoru. Proto Plán zajištění kontinuity dále zohledňuje metodiky činnosti pro případ ztráty osobních údajů v době ohrožení státu, ztrátě při teroristickém útoku⁹⁴ popřípadě při vyzrazení osobních údajů s využitím pasivního odposlechu.⁹⁵

Jak plyne z výše uvedeného, Směrnice 41. mpr pamatuje na řádné zpracování osobních údajů v souladu s ustanovením zákona č. 101/2000 Sb. a RMO č. 16/2013, ale Plán zajištění kontinuity se zaměřuje až na činnosti při vzniku mimořádných situací.

4.1.4 Shrnutí

Mechanizovaný prapor v Žatci jakožto součást bojových jednotek velitelství pozemních sil AČR je v současné době jedním z nejčastěji vyčleňovaných útvarů pro zabezpečení zahraničních operací. V průběhu roku 2018 tento útvar zabezpečoval výcvikovou misi v Mali⁹⁶ a rotní úkolové uskupení v Litvě⁹⁷, v tomto případě i včetně přípravy k její následující rotaci. I na základě výše uvedeného dochází ke stále častějšímu zpracovávání osobních údajů nejen na území České republiky, ale i daleko za jejími hranicemi.

Proto je prioritou útvaru osobní údaje chránit nejen při plnění běžné činnosti, ale i při vyslání jednotlivců do zahraničních operací, kde je riziko zneužití těchto údajů mnohem větší. Cílená edukace příslušníků 41. mpr v oblasti ochrany osobních údajů je tedy namístě, neboť případné vyzrazení „nevhodných“ informací nemusí být rizikové pouze pro ně, nýbrž i pro jejich rodinné příslušníky.

⁹³ Viz Plán zajištění kontinuity kritických činností v krizových nebo havarijních situacích.

⁹⁴ Např. uložení výbušniny či telefonická pohrůžka o jejím uložení, nález podezřelého předmětu, doručení podezřelé zásilky či přímý útok ozbrojeného pachatele nebo skupiny.

⁹⁵ Pasivním odposlechem se rozumí monitoring provozu linky či hovoru.

⁹⁶ 12. EUTM MALI (European Union Training Mission) – výcviková mise je rozmístěná v jihozápadní části Mali a cvičí vojáky ozbrojených sil, které jsou pod kontrolou legitimní malijské vlády. Hlavními úkolem mise je pomoc při výstavbě a výcviku malijské armády tak, aby byla v budoucnu schopna čelit útokům islamistických radikálů a zachovat suverenitu a teritoriální integritu země.

⁹⁷ 1. eFP Litva - rotní úkolové uskupení postavené na bázi mechanizované roty, jejíž základ tvoří jednotka s obrněnými vozidly Pandur posílená ženijní četou, logistickou jednotkou a zdravotnickým prvkem. Hlavní základna bojového uskupení se nachází ve výcvikovém prostoru litevské armády Rukla, vzdáleného cca 70 km severozápadně od Vilnius.

Zamezit všem krizovým situacím je nereálné, ale klást větší důraz na prevenci vzniku mimořádných situací již při jejich zpracování je jistě namístě. Následující kapitola proto bude zaměřena prioritně na prevenci, a to na ochranu osobních údajů již při jejich zpracování, a dále samozřejmě na rizika, tentokrát především v souvislosti s procesem zpracování osobních údajů.

4.2 Nařízení Evropského parlamentu a Rady (EU) 2016/679 v AČR, s konkrétním zaměřením na 41. mpr

4.2.1 Promítnutí Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracovávání osobních údajů v AČR

Rezort ministerstva obrany reagoval na změny spojené s nabytím účinnosti Obecného nařízení 2016/679 vyhlášením Rozkazu ministryně obrany č. 22/2018 Věstníku Zpracování a ochrana osobních údajů v rezortu Ministerstva obrany (dále jen „RMO č. 22/2018“) dne 23. května 2018. Tento právní předpis stanovuje *„v mezích vyplývajících při zpracování osobních údajů přímo z použitelného předpisu Evropské unie a z jiných právních předpisů upravujících zpracování a ochranu osobních údajů základní pravidla pro zpracování a ochranu osobních údajů organizačními celky, včetně jejich předávání subjektům mimo Ministerstvo obrany a nezbytné náležitosti smluv se zpracovateli osobních údajů.“*⁹⁸

K zabezpečení plnění povinností ministerstva obrany (dále jen „MO“) vyplývajících z právních předpisů bylo nezbytné správně nastavit práva a povinnosti uvnitř organizační struktury. Snahou RMO č. 22/2018 bylo zachování principů nastavených již v RMO č. 16/2013, grafické znázornění viz obrázek 5.

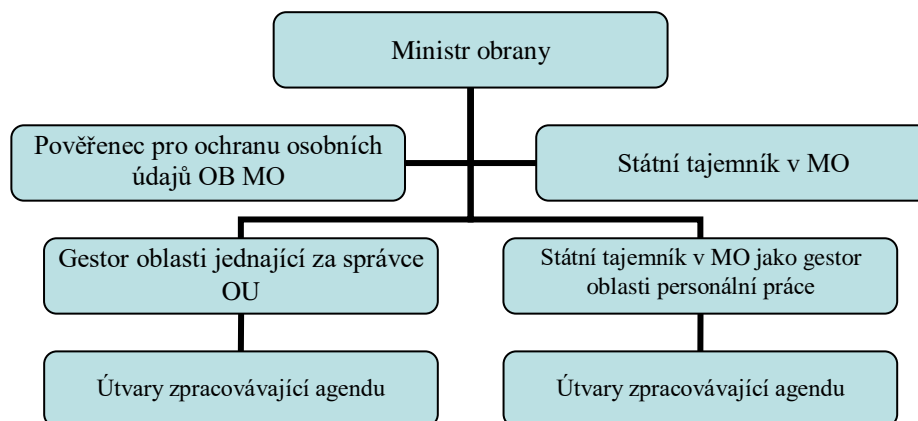
Správce⁹⁹ za MO je ministr obrany, který vnitřními předpisy stanovuje práva a povinnosti dalších vedoucích zaměstnanců. Za účelem dohledu nad systémem ochrany osobních údajů je v nezávislém postavení pověřenec pro ochranu osobních údajů. Organizačně je zařazen na Odboru bezpečnosti MO, ale může být úkolován pouze za předpokladu, že nedojde ke střetu zájmů. Jedná se o fyzickou osobu, která může být

⁹⁸ Článek 1 RMO č. 22/2018 Věstníku Zpracování a ochrana osobních údajů v rezortu Ministerstva obrany.

⁹⁹ Dle čl. 4 bod 7) Obecného nařízení 2016/679 se správcem rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení.“*

zaměstnancem správce či zpracovatele nebo může plnit úkoly na základě smlouvy o zajištění činnosti pověřence. V souvislosti s výkonem svých úkolů je vázán mlčenlivostí.

Obrázek 5 Grafické znázornění nastavení práv a povinností dle RMO č. 16/2013



Zdroj: vlastní zpracování¹⁰⁰

Metodická podpora a usměrnění v oblasti ochrany osobních údajů je svěřena státnímu tajemníkovi v MO. Dále dle čl. 3 odst. 1 RMO č. 22/2018¹⁰¹ vede souhrnnou databázi o dílčích evidencích MO zpracovávajících osobní údaje. Úkoly státního tajemníka plynou především z faktu, že pověřenec pro ochranu osobních údajů nemá kromě administrativní podpory žádnou další podporu pro výkon své činnosti, na základě čehož není schopen celou oblast metodické podpory zabezpečit. RMO č. 22/2018 mu tedy

¹⁰⁰ Smíšené postavení a režim má Vojenská policie. Ta je dle zákona č. 300/2013 Sb. o Vojenské policii a o změně některých zákonů, ve znění pozdějších předpisů, sice součástí MO, ale tento zákon jí svěřuje řadu samostatných působností. Navíc ve specifické oblasti prevence a vyšetřování trestné činnosti musí plnit úkoly vyplývající z Trestněprávní směrnice č. 2016/680. V ostatních agendách však vykonává činnosti stejného charakteru jako ostatní součásti rezortu a i Vojenská policie v nich spadá do obecné působnosti věcných gestorů a tedy i dílčích správců osobních údajů v rámci rezortu.

Zcela samostatně stojí Vojenské zpravodajství, které na základě zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů a zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, je sice součástí ministerstva vykonává veškerou svou činnost odděleně od zbývajících součástí rezortu a vystupuje tak jako samostatný správce.

¹⁰¹ Státní tajemník v ministerstvu obrany odpovídá za:

- Vedení evidence o zpracování osobních údajů v dílčích evidencích ministerstva,
- Nastavení obecných standardů ochrany osobních údajů v ministerstvu,
- Poskytování odborných konzultací a zpracování výkladových stanovisek v oblasti ochrany osobních údajů v ministerstvu. Viz čl. 3 odst. 1 RMO č. 22/2018.

svěřuje do působnosti ty úkoly, které jsou závazné z čl. 39 odst. 1 Obecného nařízení 2016/679¹⁰², ale ostatní činnost je svěřena do působnosti státního tajemníka v MO.

Nejdůležitější pravomoc svěřuje rozkaz dílčímu správci jakožto stěžejní osobě pro ochranu osobních údajů, jehož úkolem je stanovit pravidla pro zpracování osobních údajů ve své agendě. Jak stanovuje čl. 2 odst. 1 písm. a) RMO č. 22/2018¹⁰³, dílčím správcem se rozumí vedoucí organizačního celku „*jemuž organizační řád ministerstva nebo právní předpis svěřuje do působnosti výkon agendy vyžadující zpracování osobních údajů*“, popřípadě stanovil-li vedoucí organizačního celku povinnost zpracovávat osobní údaje na základě vlastního rozhodnutí. Mezi stěžejní povinnosti dílčího správce dle Obecného nařízení 2016/679 patří:

- a) stanovit účel zpracování osobních údajů a právního základů jejich zpracování;¹⁰⁴
- b) posoudit rizika hrozící subjektům údajů při zpracování osobních údajů;¹⁰⁵
- c) stanovit organizační a technická opatření k ochraně osobních údajů, jejich naplnění a pravidelné hodnocení jejich nezbytnosti a efektivnosti;
- d) zpracovávat Záznamy o činnostech zpracování osobních údajů;¹⁰⁶
- e) poskytnout součinnost pověřenci pro ochranu osobních údajů v souvislosti s plněním jeho povinností.

¹⁰² *Pověřenec pro ochranu osobních údajů vykonává alespoň tyto úkoly:*

- a) *poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o jejich povinnostech podle tohoto nařízení a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;*
- b) *monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele v oblasti ochrany osobních údajů, včetně rozdělení odpovědnosti, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;*
- c) *poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování;*
- d) *spolupráce s dozorovým úřadem a*
- e) *působení jako kontaktní místo pro dozorový úřad v záležitostech týkajících se zpracování. Viz čl. 39 odst. 1 Obecného nařízení 2016/679*

¹⁰³ *Dílčím správcem se rozumí vedoucí organizačního celku:*

1. *jemuž organizační řád ministerstva nebo právní předpis svěřuje do působnosti výkon agendy vyžadující zpracování osobních údajů,*
2. *který na základě vlastního rozhodnutí stanovil povinnost zpracovávat osobní údaje. Viz čl. 2 odst. 1 písm. a) RMO č. 22/2018.*

¹⁰⁴ Dle čl. 6 Obecného nařízení 2016/679.

¹⁰⁵ Dle čl. 35 odst. 7 Obecného nařízení 2016/679.

¹⁰⁶ Dle čl. 30 Obecného nařízení 2016/679

4.2.1.1 Promítnutí základních pojmů Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracování osobních údajů

Obecné nařízení 2016/679 přichází v souvislosti se zpracováním osobních údajů s několika novými pojmy, popřípadě k pozměnění definic pojmů původních. Pro snadnější pochopení problematiky se následující kapitola zabývá propojením základních pojmů Obecného nařízení 2016/679 se zpracováním osobních údajů v AČR.

Evidence – dle čl. 4 odst. 6) Obecného nařízení 2016/679¹⁰⁷ se jedná o „*jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.*“

V celém rezortu MO a stejně tak i v AČR je používána celá řada informačních systémů, které zpracovávají údaje k plnění určité věcné agendy. Personalisté například používají Informační systém o službě a personálu, příslušníci logistiky Informační systém logistiky a většina štábních funkcionářů útvaru denně pracuje v Elektronickém systému spisové služby (dále jen “ESSS“).

Osobní údaj – dle čl. 4 odst. 1 Obecného nařízení 2016/679¹⁰⁸ se jedná o každou informaci, na základě které lze identifikovat subjekt údajů, „*zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“

Pověřenec pro ochranu osobních údajů – i přesto, že pro Českou republiku je institut pověřence pro ochranu osobních údajů novým pojmem, v řadě evropských zemí (např. Německo či Slovensko) je již známý. Pověřenci jsou jmenováni i v centrálních evidencích Evropské unie. Pozitivní zkušenost s rolí a plněním úkolů pověřence pravděpodobně vedla k jejich převzetí do Obecného nařízení 2016/679.¹⁰⁹ Do funkce pověřence musí být fyzická osoba jmenována ministerstvem jako orgánem veřejné moci.

¹⁰⁷ Evidenci se rozumí „*jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.*“ Viz čl. 4 odst. 6) Obecného nařízení 2016/679.

¹⁰⁸ Osobními údaji se rozumí „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“ Viz čl. 4 odst. 1 Obecného nařízení 2016/679.

¹⁰⁹ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 102.

Jak se uvádí výše, místo pověřence pro ochranu osobních údajů bylo zřízeno systemizací na Odboru bezpečnosti MO. Pro potřeby Vojenské policie je ovšem nutné zřízení samostatného pověřence, a to na základě ustanovení Směrnice Evropského parlamentu a Rady (EU) 2016/680 (blíže v kapitole 3.2.3). Postavení pověřence v oblasti trestné činnosti je na podobné úrovni jako postavení pověřence pro ochranu osobních údajů dle Obecného nařízení 2016/679.

Profilování – jedná se o nový pojem, který je v ustanovení čl. 4 odst. 4 Obecného nařízení 2016/679¹¹⁰ definován jako „*jakákoliv forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě.*“ Jedná se zejména o rozборы nebo odhady týkající se pracovní výkonnosti, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti či chování.

V dnešní pokrokové době se pro zjednodušení práce využívá nejnovějších informačních systémů, u kterých dochází k celé řadě automatizovaných operací.¹¹¹ Dle Obecného nařízení 2016/679 je za profilování ovšem považována pouze taková operace, která automaticky bez zásahu fyzických osob na základě nastavených kritérií zpracuje hodnocení dat o osobě včetně předběžného závěru. Za příklad profilování v rámci AČR lze považovat systém samostatně vyhodnocující chování zaměstnanců na síti, které následně na jejich problematické chování upozorňuje.

Příjemce – oproti strohé definici pojmu uvedené v zákoně č. 101/2000 Sb.,¹¹² přichází Obecné nařízení 2016/679 v čl. 4 odst. 9¹¹³ s vysvětlením, že za příjemce se považuje „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli.*“

¹¹⁰ Profilováním se rozumí „*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.*“ Viz čl. 4 odst. 4 Obecného nařízení 2016/679.

¹¹¹ Například výpočet platu či přeměrování elektronického dokumentu předem určeným osobám.

¹¹² Příjemcem se rozumí „*každý subjekt, kterému jsou osobní údaje zpřístupněny.*“ Viz §4, odst. 1 písm. o) zákona č. 101/2000 Sb., o ochraně osobních údajů.

¹¹³ Příjemcem se rozumí „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli. Avšak orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem členského státu, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly ochrany údajů pro dané účely zpracování.*“ Viz v čl. 4 odst. 9 Obecného nařízení 2016/679.

Příjemcem tedy jsou všechny subjekty, kterým jsou předány některou součástí AČR osobní údaje, a to na základě smluvního vztahu nebo v souladu s právním předpisem. Příkladem role příjemce v AČR může být například poskytovatel jazykového vzdělávání či rekvalifikačních kurzů.¹¹⁴

Pseudonymizace – je definována v čl. 4 odst. 5 Obecného nařízení 2016/679¹¹⁵ jako zpracování osobních údajů takovým způsobem, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací. Tyto dodatečné informace musí být „*uchovány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.*“ Pattynová k tomu dodává, že „*taková úprava dat znemožňuje jejich přiřazení ke konkrétní fyzické osobě bez odděleně uchovaného klíče.*“¹¹⁶ Právě možnost přiřazení dodatečných informací sloužících k identifikaci osoby odlišuje pseudonymizované údaje od anonymních. Vazba mezi subjektem údajů a informacemi je totiž u anonymních údajů nenávratně odstraněna.

Příkladem z praxe AČR je využití osobních údajů vojáků z povolání pro potřeby stanovení pořadí vojáků pro kariérní růst.¹¹⁷ Jedná se o proces, při kterém jsou členům komise předkládány skutečná data o průběhu služby konkrétních vojáků, ale není zde uvedeno jméno a příjmením, pouze vygenerovaný číselný kód. Až po ukončení činnosti komise jsou kódy propojeny s jednotlivci a výsledky poté předány k rukám personalistů. Rozdíl mezi osobními, anonymními a pseudonymizovanými údaji znázorňuje tabulka 9.

V prvním řádku jde o osobní údaje v celém rozsahu. Jelikož lze identifikovat fyzickou osobu, je nutné za osobní údaje považovat i další údaje k ní přiřazené (vzdělání, délku praxe apod.). Za předpokladu, že správce nevratně odstraní jméno, příjmení a osobní číslo (jak uvádí druhý řádek), údaje získají přívlastek anonymní. Podmínkou ovšem je, že skutečně došlo k likvidaci dat a opětovná identifikace již není možná. Třetí řádek

¹¹⁴ Rekvalifikační kurz umožňuje příslušníkům AČR získat novou kvalifikaci nebo rozšířit stávající kvalifikaci před zánikem jejich služebního poměru.

¹¹⁵ Pseudonymizací se rozumí „*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.*“ Viz v čl. 4 odst. 5 Obecného nařízení 2016/679.

¹¹⁶ PATTYNOVÁ, J. a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář.* 2018, s. 55.

¹¹⁷ RMO č. 9/2017 Stanovení pořadí vojáků z povolání pro realizaci personálních opatření systému řízení kariér, ve znění pozdějších předpisů.

je ukázkou pseudonymizace, kdy tmavě podbarvené údaje lze považovat za pseudonymizované, pokud ovšem dílčí správce uchová světle podbarvené údaje odděleně (například zašifrovaně) a pro své potřeby dále používá pouze tmavě podbarvená data doplněná číselným kódem (např. 0001, 0002 atd.)¹¹⁸.

Tabulka 9 Rozdíl mezi osobním, anonymním a pseudonymizovaným údajem

Jméno	Příjmení	Osobní číslo	Vzdělání	Délka praxe	Jazykové předpoklady	Kvalifikační předpoklady
Karel	Nový	2059267	VŠ – Ing.	18	AJ 2222	Kurz vyšších důstojníků
			<u>VŠ – Ing.</u>	<u>18</u>	<u>AJ 2222</u>	<u>Kurz vyšších důstojníků</u>
Karel	Nový	2059267	VŠ – Ing.	18	AJ 2222	Kurz vyšších důstojníků

Legenda: osobní údaje, anonymní údaje, - pseudonymizované údaje, - 0001

0001	VŠ – Ing.	18	AJ 2222	Kurz vyšších důstojníků
------	-----------	----	---------	-------------------------

Zdroj: vlastní zpracování

Subjekt údajů – jak vychází z definice osobního údaje v čl. 4 odst. 1 Obecného nařízení 2016/679, představuje přesně identifikovanou či identifikovatelnou fyzickou osobu, „*kteřou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“ Konkrétně lze tedy za subjekt údajů považovat žijícího člověka, kterého dané údaje umožňují přesně určit, popřípadě ho lze identifikovat z údajů propojených za užití běžně dostupných prostředků a informací.¹¹⁹

Ve vztahu k AČR jsou za subjekty údajů považovány osoby působící v rezortu MO v současnosti či minulosti, dále osoby, které se obrátí na některou součást rezortu a v neposlední řadě zástupci smluvních partnerů, mezinárodních organizací apod.

Je-li subjektem údajů zaměstnanec, voják v činné službě nebo voják zařazený v aktivní záloze, komunikuje s ním příslušný vedoucí organizačního celku¹²⁰. Je-li subjektem zástupce smluvního partnera, komunikuje s ním zaměstnanec rezortu určený

¹¹⁸ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 42, 43.

¹¹⁹ Specifickým případem jsou osoby samostatně výdělečně činné, které při své podnikatelské činnosti vystupují jako fyzické, čímž dochází k prolínání obou postavení.

¹²⁰ U aktivních záloh navíc dochází ke komunikaci s ředitelem příslušného Krajského vojenského velitelství.

v uzavřené smlouvě a v případě jiných osob je v této oblasti kompetentní osobou pověřenec pro ochranu osobních údajů.

Zpracovatel – dle čl. 4 odst. 8 Obecného nařízení 2016/679¹²¹ je za zpracovatele považována „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“

V souvislosti s AČR tím pádem půjde o fyzickou či právnickou osobu, se kterou rezort MO uzavřel smluvní vztah, na jehož základě od něj bude zpracovatel přebírat osobní údaje a po provedení stanovených činností je vrátí zpět správci.

4.2.1.2 Dodržování zásad zpracování osobních údajů

Zásady zpracování osobních údajů lze označit jako základ, na němž je celé Obecné nařízení 2016/679 postaveno. Většina zásad vychází z jednotlivých povinností uvedených v předchozí Směrnici 95/46/ES, resp. v zákoně č. 101/2000 Sb., ale Obecné nařízení 2016/679 v čl. 5 odst. 1 přináší inovaci v jejich vyjmenování. Konkrétně se jedná se o zásady:

- zákonnosti, korektnosti a transparentnosti;
- účelového omezení;
- minimalizace údajů;
- přesnosti;
- omezení uložení;
- integrity a důvěrnosti;
- zodpovědnosti.

Uvedené zásady, které Žůrek výstižně nazývá „zevšeobecněným vyjádřením dílčích povinností“¹²², musí AČR zohlednit v pravidlech pro zpracování osobních údajů v jednotlivých evidencích, z čehož plyne nutnost s nimi počítat již od samotného záměru zpracovávat osobní údaje.

Za nejdůležitější zásadu lze považovat zásadu zákonnosti, neboť ke zpracování osobních údajů může správce přistoupit pouze v případě, má-li k takovému zpracování

¹²¹ Zpracovatelem se rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce“. Viz čl. 4 odst. 8 Obecného nařízení 2016/679.

¹²² ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 58.

alespoň jeden právní důvod.¹²³ V podmínkách AČR se bude ve většině případů jednat o zpracování osobních údajů na základě plnění povinnosti stanovené zákonem, popřípadě na základě smluvního vztahu. V menším zastoupení se bude jednat o zpracování osobních údajů na základě vydání souhlasu subjektu údajů.

Se zásadou účelového omezení souvisí uchovávání osobních údajů pouze na dobu nezbytnou, odpovídající účelu zpracování. V rezortu MO tuto problematiku řeší RMO č. 34/2017 Věstníku Spisový řád Ministerstva obrany, který obsahuje spisový a skartační plán. Jedná se o právní předpis uvádějící skartační lhůty pro všechny druhy dokumentů zpracovávané v rámci rezortu. Úkolem dílčího správce by v rámci posuzování dopadů zpracování osobních údajů mělo být prověření, zda skartační lhůty korespondují s lhůtami uvedenými v právních předpisech a zda jsou pro konkrétní typy dokumentů lhůty stanoveny.

Oprávněné zničení dokumentů obsahujících osobní údaje se prokazuje na základě protokolu o provedeném skartačním řízení či protokolem o provedení výběru archiválií mimo skartační řízení. Archivy mají pravomoc ukládat trvale dokumenty označené za archiválie včetně těch, které obsahují osobní údaje živých osob.¹²⁴

Se zásadou omezení účelu úzce souvisí zásada minimalizace údajů, která správci brání, aby od subjektů údajů požadoval více informací, než je nezbytně nutné. Jak uvádí ustanovení čl. 25 Obecného nařízení 2016/679¹²⁵, hlavním cílem záměrné a standardní

¹²³ Viz čl. 6 odst. 1 Obecného nařízení 2016/679:

- a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- b) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- c) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje;
- d) zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby;
- e) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- f) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

¹²⁴ Viz čl. 17 (Právo na výmaz) a čl. 89 (Záruky a odchylky týkající se zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely) Obecného nařízení 2016/679.

¹²⁵ Článek 25 Obecného nařízení 2016/679 – Záměrná a standardní ochrana osobních údajů

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.

ochrany osobních údajů je minimalizace rizik souvisejících se zpracováním. Proto správci dále ukládá povinnost zavést vhodná organizační a technická opatření sloužící k eliminaci rizik. Zohlednit je nutné množství shromážděných osobních údajů, rozsah jejich zpracování či dobu uložení.

Pro přehlednost a shrnutí hlavních zásad slouží tabulka 10, která kromě stručného popisu principů zahrnuje i dopady, které zavedení Obecného nařízení 2016/679 přináší.

Tabulka 10 Zásady zpracování osobních údajů

Zásada	Stručný popis	Dopad
Zákonnost, korektnost, transparentnost	Správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně.	Zásady ukládají organizacím rozšířenou povinnost v oblasti dodržování předpisů a klade důraz na zvýšení jejich péče při vytváření a zavádění činností v oblasti zpracování osobních údajů.
Omezení účelu	Osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely.	Nařízení přináší omezené změny. Další zpracování osobních údajů pro archivaci, vědecké, historické či statistické účely je stále povoleno, ale podléhá dodatečným zárukám. ¹²⁶
Minimalizace údajů	Osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány.	Povinnost zajistit, aby osobní údaje nepřesáhly míru, je nahrazena povinností zajistit, aby osobní údaje byly omezeny na nezbytný rozsah.
Přesnost	Osobní údaje musí být přesné.	Princip přesnosti se nemění, nařízení pouze blíže upřesňuje povinnost, že vymazání nebo náprava nepřesných údajů musí být provedena neprodleně.
Omezení uložení	Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány.	Souvislost s „právem být zapomenut“, dle kterého mají subjekty údajů právo na vymazání osobních údajů, a to v některých případech i dříve, než uplyne maximální doba uchování údajů.
Integrita a důvěrnost	Technické a organizační zabezpečení osobních údajů.	Samotný princip je v podstatě nezměněn, dochází pouze k posílení myšlenky, že zabezpečení dat je základní povinností všech správců.

Zdroj: zpracováno dle NEZMAR, L. *GDPR: Praktický průvodce implementací*. 2017, s. 33, 50 a 51.

2. Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti. Tato opatření zejména zajistí, aby osobní údaje nebyly standardně bez zásahu člověka zpřístupněny neomezenému počtu fyzických osob.

¹²⁶ Viz čl. 89 Obecného nařízení 2016/679.

Rozvinutí jednotlivých zásad zpracování je uvedeno v čl. 5 odst. 1 Obecného nařízení 2016/679. Dodržování stanovených zásad je pro správce zásadní nejen z důvodu, že se jedná zároveň i o jeho povinnosti, ale také proto, že správce má nově povinnost být schopen dodržování těchto zásad doložit.¹²⁷ K prokazování souladu s uvedenými zásadami budou sloužit Záznamy o činnostech zpracování¹²⁸ a dále kodexy a osvědčení.¹²⁹

4.2.1.3 Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů a s tím v některých případech související povinná konzultace s dozorovým orgánem jsou dva nové instituty, které ve Směrnici 95/46/ES či zákoně č. 101/2000 Sb. doposud nebyly zohledněny. Jak stanoví čl. 35 odst. 1 Obecného nařízení 2016/679¹³⁰ správce či zpracovatel posouzení vlivu na ochranu osobních údajů provádí pouze v případech, představuje-li zpracování vysoké riziko pro práva a svobody fyzických osob.

Jelikož vybraný útvar provádí pouze běžné, nerizikové zpracování, posouzení vlivu na ochranu osobních údajů není povinen provádět. Činnosti plynoucí z pravděpodobnosti vysokých rizik při zpracování jsou obsaženy v příloze 1 Posouzení vlivu na ochranu osobních údajů.

4.2.1.4 Zajišťování ochrany osobních údajů

Základními pravidly zabezpečení ochrany osobních údajů se zabývá část třetí RMO č. 22/2018. Kromě základních povinností zaměstnanců při zpracování osobních údajů¹³¹ se dále zaměřuje na problematiku označování dokumentů, pořizování kopií či zvláštnosti pro zpracování osobních údajů.

¹²⁷ Viz čl. 5 odst. 2 Obecného nařízení 2016/679.

¹²⁸ Viz recitál 82 Obecného nařízení 2016/679 - *Aby správce nebo zpracovatel doložil soulad s tímto nařízením, měl by vést záznamy o činnostech zpracování, za které odpovídá. Každý správce a zpracovatel by měl být povinen spolupracovat s dozorovým úřadem a na jeho žádost mu tyto záznamy zpřístupnit, aby na jejich základě mohly být tyto operace zpracování monitorovány.*

¹²⁹ NEZMAR, L. *GDPR: Praktický průvodce implementací*. 2017, s. 33.

¹³⁰ *Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení. Viz čl. 35 odst. 1 Obecného nařízení 2016/679.*

¹³¹ Článek 9 RMO č. 22/2018.

V porovnání s RMO č. 16/2013 jsou povinnosti uvedené v čl. 10, 11 a 12 RMO č. 22/2018 téměř totožné, za zmínku ale stojí odlišné pojetí povolení označovat elektronický soubor osobním číslem zaměstnance, což předchozí předpis neumožňoval. V novém rozkaze dostává větší prostor problematika týkající se povinností zaměstnanců při přístupu subjektů mimo rezort k osobním údajům. Zde bude stěžejní odlišit zpracování osobních údajů rezortu MO vnějším subjektem od případů, kdy dochází k předávání údajů jinému správci. Oba tyto druhy zpracování mají shodnou podmínku uvedenou v čl. 13 odst. 1 RMO č. 22/2018¹³², a to že zpřístupnění je možné pouze v případě, stanoví-li tak právní předpis nebo smlouva. Jak plyne z praxe, v rezortu MO se bude jednat spíše o případy podílu jiného subjektu na zpracování osobních údajů. K výše uvedenému čl. 28 Obecného nařízení 2016/679 požaduje následující:

- *správce pro zpracování využije pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření;*
- *zpracovatel nesmí bez písemného povolení správce zapojit do zpracování žádné další zpracovatele. V případě písemného povolení je zpracovatel povinen správce informovat o všech zamýšlených změnách, čímž poskytne správci příležitost vznést vůči těmto změnám námitky;*
- *ve sjednané smlouvě či jiném právním aktu zavazujícím zpracovatele vůči správci¹³³ musí být vymezen především předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů, kategorie subjektů údajů a v neposlední řadě povinnosti a práva správce.¹³⁴*

4.2.1.5 Povinnosti při zjištění porušení zabezpečení osobních údajů

Porušením zabezpečení osobních údajů Obecné nařízení 2016/679 popisuje stav, který „vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních

¹³² Zpřístupnit zpracované osobní údaje subjektu mimo ministerstvo nebo je předat jinému správci je možné jen pokud to stanoví právní předpis nebo smlouva. Viz čl. 13, odst. 1 RMO č. 22/2018.

¹³³ Smlouva nebo jiný právní akt musí být vyhotoveny písemně, v to počítaje i elektronickou formu. Viz čl. 28 odst. 9 Obecného nařízení 2016/679.

¹³⁴ Článek 28 odst. 1, 2 a 3 Obecného nařízení 2016/679.

údajů.¹³⁵ V souvislosti s výše uvedeným zavádí Obecné nařízení 2016/679 dvě nové povinnosti, a to ohlášení porušení zabezpečení dozorovému úřadu a subjektu údajů.

Pro potřeby rezortu MO je za určitého prostředníka mezi dílčím správcem a dozorovým orgánem stanoven pověřenec. Tomu je dílčí správce povinen porušení zabezpečení bezodkladně předat (včetně možného vzniku rizika) a povinností pověřence je poté zjištěnou informaci posoudit.¹³⁶ Z tohoto důvodu RMO č. 22/2018 neumožňuje 72 hodinovou lhůtou dílčímu správci, nýbrž pověřenci, a to k posouzení jemu předaných informací.

Ohlašovací povinnost vůči dozorovému úřadu vzniká za předpokladu, dojde-li k takovému porušení zabezpečení osobních údajů, které představuje riziko pro práva a svobody fyzických osob. Porušení musí být ohlášeno bez zbytečného odkladu, pokud možno do 3 dnů od zjištění porušení zabezpečení, a musí obsahovat následující informace:

- a) *popis povahy daného případu porušení včetně kategorií a přibližného počtu dotčených subjektů údajů a kategorií a přibližného množství dotčených záznamů osobních údajů;*
- b) *jméno a kontaktní údaje pověřence nebo jiného kontaktního místa, které může poskytnout bližší informace;*
- c) *popis pravděpodobných důsledků porušení;*
- d) *popis opatření, která správce přijal nebo navrhl k přijetí s cílem vyřešit dané porušení, včetně případných opatření ke zmírnění možných nepříznivých dopadů.¹³⁷*

Není-li možné doložit všechny požadované informace současně, nabízí Obecné nařízení 2016/679 možnost poskytnutí informací postupně, ale bez dalšího zbytečného odkladu.¹³⁸

Obecné nařízení 2016/679 dále stanovuje, že v případech porušení zabezpečení osobních údajů, u kterých je pravděpodobné, že budou mít za následek vysoké riziko pro práva a svobody fyzických osob, je povinností správce toto porušení bez zbytečného

¹³⁵ Článek 4 odst. 12 Obecného nařízení 2016/679.

¹³⁶ *Dojde-li k porušení zabezpečení osobních údajů je dílčí správce povinen bezodkladně předat informaci o tomto porušení a možném vzniku rizika pověřenci, a to ve formátu stanoveném pro tyto účely Úřadem. Viz čl. 15 odst. 1 RMO č. 22/2018.*

¹³⁷ Článek 33 odst. 3 Obecného nařízení 2016/679.

¹³⁸ Článek 33 odst. 4 Obecného nařízení 2016/679.

odkladu oznámit subjektu údajů.¹³⁹ V AČR tato povinnost opět připadá na pověřence po jeho řádném posouzení daného incidentu.

Vzhledem k podmínce vysokého rizika pro práva a svobody fyzických osob by v rezortu MO k ohlašování případů přímo subjektům údajů mělo docházet pouze v ojedinělých případech¹⁴⁰, přesto by zájmem správců měla být snaha o jejich předcházení především za pomoci bezpečnostních opatření. V obou případech potvrzeného porušení zabezpečení osobních údajů na základě posouzení pověřencem je jeho povinností informovat ministra obrany a státního tajemníka v MO, a to ještě před samotným podáním oznámení dozorovému úřadu.¹⁴¹

K prevenci před opakováním porušení zabezpečení osobních údajů slouží vyhodnocení příčin a přijetí potřeby změnit stanovená organizační a technická opatření popř. důslednější vynucení opatření již přijatých. V souvislosti s tím je dílčí správce povinen bezodkladně zapracovat přijatá opatření do Záznamů o činnostech zpracování osobních údajů včetně příslušné úpravy organizačních a technických opatření.¹⁴²

4.2.1.6 Povinnosti správce vůči subjektu údajů

Práva subjektů údajů jsou v porovnání se Směrnicí 95/46/ES, resp. se zákonem č. 101/2000 Sb., v novém právním rámci upravena podrobněji. Kromě již známých práv např. právo na informace, právo na přístup k údajům či na jejich opravu, přichází zcela nová práva, a to právo na přenositelnost či „právo být zapomenut“. K právu na přenositelnost Janečková uvádí *„toto právo vzbudilo mnoho emocí. Přenositelnost údajů subjektům údajů v podstatě umožňuje získat a opětovně používat "své" údaje pro své vlastní účely a napříč různými službami. Toto právo usnadňuje schopnost snadno a bez zábran přesouvat, kopírovat nebo předávat osobní údaje z jednoho informačního prostředí do jiného.“*¹⁴³

¹³⁹ Článek 34 odst. 1 Obecného nařízení 2016/679.

¹⁴⁰ Jedná se o takový bezpečnostní incident, který by výrazně poškodil subjekt údajů na jeho právech (např. podporující diskriminaci jednotlivce).

¹⁴¹ Před podáním oznámení Úřadu nebo subjektu údajů informuje pověřenec o porušení ministra obrany a státního tajemníka v ministerstvu. Viz čl. 15 odst. 4 RMO č. 22/2018.

¹⁴² Dílčí správce bezodkladně zabezpečí zpracování přijatých opatření do záznamů o činnostech zpracování osobních údajů a příslušnou úpravu organizačních a technických opatření k ochraně osobních údajů. Článek 17 odst. 3 RMO č. 22/2018.

¹⁴³ JANEČKOVÁ, E. *GDPR. Praktická příručka implementace*. 2018, s. 24.

Právo být zapomenut resp. právo na výmaz nově umožňuje subjektu údajů „požádat o vymazání či odstranění osobních údajů, a to bez ohledu na to, zda existuje nějaký přesvědčivý důvod pro jeho další zpracování.“¹⁴⁴ Jak uvádí Obecné nařízení 2016/679, nejedná se ovšem o právo absolutní, neboť ke smazání osobních údajů musí být splněn alespoň jeden z důvodů uvedených v čl. 17 odst. 1.¹⁴⁵ Zabezpečení řádného výkonu výše uvedených práv je nezbytné pro soulad zpracování osobních údajů jako celku s Obecným nařízením 2016/679.¹⁴⁶

Ministerstvo obrany, jakožto správce, je na základě ustanovení dle čl. 12 odst. 1 Obecného nařízení 2016/679¹⁴⁷ povinno přijmout taková opatření, aby poskytlo „subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v člancích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování.“¹⁴⁸ Podání

¹⁴⁴ NEZMAR, L. *GDPR: Praktický průvodce implementací*. 2017, s. 87.

¹⁴⁵ *Subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud je dán jeden z těchto důvodů:*

- a) *osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány;*
- b) *subjekt údajů odvolá souhlas, na jehož základě byly údaje podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) zpracovány, a neexistuje žádný další právní důvod pro zpracování;*
- c) *subjekt údajů vznese námitky proti zpracování podle čl. 21 odst. 1 a neexistují žádné převažující oprávněné důvody pro zpracování nebo subjekt údajů vznese námitky proti zpracování dle čl. 21 odst. 2;*
- d) *osobní údaje byly zpracovány protiprávně;*
- e) *osobní údaje musí být vymazány ke splnění právní povinnosti stanovené v právu Unie nebo členského státu, které se na správce vztahuje;*
- f) *osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1. Viz čl. 17 odst. 1 Obecného nařízení 2016/679.*

¹⁴⁶ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 124.

¹⁴⁷ *Správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace uvedené v člancích 13 a 14 a učinil veškerá sdělení podle článků 15 až 22 a 34 o zpracování, zejména pokud se jedná o informace určené konkrétně dítěti. Informace poskytne písemně nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby. Viz čl. 12 odst. 1 Obecného nařízení 2016/679.*

¹⁴⁸ Článek 13 Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů; čl. 14 Informace poskytované v případě, že osobní údaje nebyly získány od subjektu údajů; čl. 15 Právo subjektu údajů na přístup k osobním údajům; čl. 16 Právo na opravu; čl. 17 Právo na výmaz; čl. 18 Právo na omezení zpracování; čl. 19 Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování; čl. 20 Právo na přenositelnost údajů; čl. 21 Právo vznést námitku; čl. 22 Automatizované individuální rozhodování, včetně profilování a čl. 34 Oznamování případů porušení zabezpečení osobních údajů subjektu údajů.

informací musí být provedeno písemně¹⁴⁹ bez zbytečného odkladu, maximální lhůta činí 1 měsíc od obdržení žádosti.

Nejčastěji lze očekávat žádosti týkající se práva subjektu údajů na přístup ke zpracovaným osobním údajům, které dle čl. 15 odst. 1 Obecného nařízení 2016/679 mohou obsahovat následující dotazy:

- jaké údaje o subjektu údajů jsou v dokumentech zpracovávány;
- pro jaký účel a v jakém rozsahu;
- na základě jakého titulu dochází ke zpracování;
- po jakou dobu budou údaje uloženy.

Rozkaz MO č. 22/2018 reaguje na výše uvedené pomocí ustanovení čl. 18 a 19, kde jako stěžejní informaci uvádí, že komunikaci mezi subjektem údajů a správcem, tedy ministrem obrany, zabezpečuje pouze pověřenec a dále jaké jsou v této souvislosti jeho povinnosti a pravomoci.

4.2.2 Promítnutí Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracování osobních údajů u 41. mpr

4.2.2.1 Promítnutí základních pojmů Nařízení Evropského parlamentu a Rady (EU) 2016/679 do činnosti 41. mpr

Následující kapitola je zaměřena na propojení stěžejních pojmů Obecného nařízení 2016/679 s praktickým příkladem vazby k činnosti u 41. mpr.

Evidence – jak již bylo uvedeno (blíže v kapitole 4.2.1.1), s pojmem „evidence“ souvisí používání různých informačních systémů ke zpracování určité agendy. Stejně tak je tomu i u 41. mpr, kde za dobu jejich využívání došlo v řadě systémů k určitému rozšiřování o další moduly zpracovávající jiné agendy. V současné době jsou v rámci jednoho informačního systému 41. mpr zpracovávány údaje i k několika účelům.¹⁵⁰

¹⁴⁹ Nebo jinými prostředky, včetně ve vhodných případech v elektronické formě. Pokud si to subjekt údajů vyžádá, mohou být informace poskytnuty ústně, a to za předpokladu, že identita subjektu údajů je prokázána jinými způsoby.

¹⁵⁰ Příklad z praxe – za jednu z evidencí osobních údajů by mohl být označen ESSS. V rámci tohoto systému však funguje modul úkolů, který je zřízen k evidenci služebních úkolů a sledování jejich plnění. Jedná se o evidenci, která je zčásti propojena s dokumenty v ESSS, ale část úkolů vzniká nezávisle na dokumentech procházejících spisovou službou. Tato evidence obsahuje osobní údaje (jméno, příjmení, zařazení, služební emailová adresa), které se strukturovaně zpracovávají. Jedná se tedy o evidenci osobních údajů, která je ale vedena za jiným účelem, než je spisová služba. Dle Obecného nařízení 2016/679 by tedy měla být označena za samostatnou evidenci osobních údajů.

Osobní údaj – jedná se pojem, u kterého veškerá problematika Obecného nařízení 2016/679 začíná i končí. S osobními údaji se sekáváme každý den a ne vždy jsme schopni najít souvislosti s jejich možným zneužitím neoprávněnou osobou. Z praxe u 41. mpr lze říct, že za osobní údaj je možné považovat i informace o vydané výstroji konkrétnímu vojákovi či data uvedená na průkazu k povolení vjezdu do objektu kasáren jednotlivců. Pokud ovšem u těchto údajů dojde k oddělení identifikátoru osoby, charakter osobního údaje pomine.

Příjemce – nejčastěji využívaným příjemcem u vybraného útvaru je poskytovatel jazykového vzdělávání. Jelikož jsou příslušníci praporu na základě stanovených odborných požadavků jednotlivých služebních míst povinni splnit danou jazykovou úroveň STANAG 6001¹⁵¹, bývá pro tyto potřeby uzavřen smluvní vztah k zabezpečení jazykové přípravy. Poskytovateli jazykového vzdělávání jsou za tímto účelem předány informace ohledně kontaktní osoby odpovědné za zabezpečení plnění smlouvy a dále pak osobní údaje ohledně jednotlivců, kterým bude vzdělání poskytováno. Poskytovatel jazykového vzdělání zpracuje údaje za vlastním účelem a na vlastní odpovědnost jako samostatný správce. Výstupem pro 41. mpr je poté pouze informace ohledně účasti na daném školení a dosažený výsledek.

Zpracovatel – příkladem subjektu u 41. mpr, který zpracovává osobní údaje pro správce, může být firma zabezpečující ochranu vojenských objektů.¹⁵² Na základě sjednaného vztahu mezi rezortem a smluvním parterem dochází k identifikaci osob vstupujících do vojenských objektů a zpracování záznamu o tomto pobytu. Výstup z této činnosti poté zpracovatel předává 41. mpr k dalšímu zpracování či uložení.

4.2.2.2 Vliv na běžnou činnost 41. mpr

Nabytí účinnosti Obecného nařízení 2016/679 se v činnosti 41. mpr zásadním způsobem nepromítlo. Jelikož v té době byla veškerá agenda spojená se zpracováním osobních údajů realizována v souladu s RMO č. 16/2013 a u útvaru docházelo a stále

¹⁵¹ STANAG 6001 (zkratka z angl. Standardization Agreement - Standardizační dohoda) - jazyková zkouška poskytující základ pro testování dovedností zaměstnanců ve strukturách organizace NATO, armádách členských států NATO a Partnerství pro mír.

¹⁵² V případě 41.mpr se jedná o firmu Vojenské lesy a statky České republiky. Jedná se o státní podnik, který je účelovou organizací založenou Ministerstvem obrany České republiky. Hospodaří na státních pozemcích jak v existujících vojenských újezdech, tak i v některých zrušených vojenských prostorech.

dochází pouze k běžnému, nerizikovému zpracování osobních údajů, lze konstatovat, že útvar byl na nabytí účinnosti Obecného nařízení 2016/679 z větší části připraven.

Nejvíce se evropská právní úprava promítla do činnosti skupin personální, ekonomické a skupiny ochrany utajovaných informací a dále všech uživatelů elektronického systému spisové služby. V souladu s RMO č. 22/2018 a s pokyny z Metodických dnů organizovaných nadřízeným stupněm došlo k okamžitému zákazu označování ukládaných dokumentů v digitální podobě osobními údaji¹⁵³ a dále k pořizování a uchovávání kopií osobních dokladů, u kterých vedoucí organizačního celku jednoznačně nestanovil jejich nezbytnost.¹⁵⁴

V návaznosti na vyhlášení RMO č. 22/2018 došlo u 41. mpr k mimořádnému školení zaměstnanců, kteří mají na základě Směrnice 41. mpr a dodatku v popisu funkční náplně povoleno zpracování osobních údajů s prioritním zaměřením na část třetí RMO č. 22/2018.¹⁵⁵ Seznámení s problematikou a její pochopení bylo stvrzeno podpisem jednotlivých zaměstnanců v prezenční listině. Pro příslušníky ekonomické skupiny útvaru bylo prostřednictvím Finančního informačního systému¹⁵⁶ (dále jen „FIS“) distribuováno Upřesnění práce s osobními údaji v účetních evidencích FIS (viz Příloha B) se zaměřením na konkrétní příklady osobních údajů, které byly v rámci analýzy údajů v jednotlivých modulech zjištěny. Personální skupina byla poučena v rámci Metodického dne organizovaného nadřízeným stupněm, přičemž za stěžejní změnu považují zákaz označování dokumentů ukládaných v digitální podobě osobním údajem, a to v souladu

¹⁵³ Při ukládání dokumentů v digitální podobě, včetně datových zpráv, je zakázáno v označení ukládaného souboru používat osobní údaje s výjimkou osobního čísla. Při označování předmětu dokumentu nebo spisu v elektronickém systému spisové služby nebo při jejich doručování cestou elektronických komunikací se věta první použije obdobně. Stejně je zakázáno zpracování osobních údajů v metadatech dokumentů v digitální podobě. Viz čl. 10 odst. 1 RMO 22/2018.

¹⁵⁴ Pokud dílčí správce stanoví, že je nezbytné ke splnění účelu určité agendy pořizování a uchovávání kopií občanského průkazu nebo cestovního dokladu, stanoví současně podmínky pro získání písemného souhlasu držitele osobního dokladu a jeho uchovávání po celou dobu zpracování kopie dokladu. Viz čl. 11 RMO č. 22/2018.

¹⁵⁵ Článek 8 Nastavení standardů ochrany osobních údajů v dílčích evidencích, čl. 9 Povinnosti zaměstnanců při zpracování osobních údajů, čl. 10 Označování ukládaných dokumentů v digitální podobě, čl. 11 Pořizování kopií osobních dokladů, čl. 12 Zvláštnosti pro zpracování osobních údajů při elektronickém zpracování a při zpracování audiovizuálních dokumentů a čl. 13 Povinnosti zaměstnanců při přístupu subjektů mimo rezort k osobním údajům. Viz část třetí RMO 22/2018.

¹⁵⁶ Systém, jehož účelem je zabezpečení informační podpory při řízení a realizaci finančního zabezpečení rezortu MO. Zahrnuje ekonomické agendy, řízení oběhu dokumentů prostřednictvím spisové služby, řadu registrů a správních agend včetně softwarového řešení vedení správního řízení. K dispozici má řadu specifických modulů pro podporu činností státních a samosprávních úřadů.

s čl. 10 odst. 1 RMO č. 22/2018.¹⁵⁷ Skupina ochrany informací v rámci pravidelných školení příslušníkům 41. mpr zdůraznila rizika plynoucí z neopatrného nakládání s osobními údaji především v souvislosti s používáním mobilních zařízení a sociálních sítí. Na základě poznatků ze Zpravodajské informace pro Náčelníka generálního štábu AČR¹⁵⁸, byla totiž identifikována vysoká míra rizika spočívající v různých formách možného zneužití především těch informací, které sami příslušníci AČR poskytují na sociálních sítích.

4.2.3 Shrnutí

Šetřením u vybraného útvaru bylo zjištěno, že na základě plnění ustanovení RMO č. 16/2013 byly základy ochrany osobních údajů vhodně nastaveny a nyní pouze dochází, vlivem implementace Obecného nařízení 2016/679, k vytvoření jejich nastavby. Dnem nabytí účinnosti evropského nařízení došlo zároveň k vyhlášení RMO č. 22/2018, který nové oblasti ochrany při zpracování osobních údajů upřesňuje pro podmínky rezortu MO.

I přesto, že Obecné nařízení 2016/679 v čl. 2 stanovuje, že „*se nevztahuje na zpracování osobních údajů prováděné při výkonu činností, které nespádají do oblasti působnosti práva Unie*“¹⁵⁹, rezort MO se plnění jeho ustanovení nevyhýbá. Tuhle myšlenku podporuje i fakt, že v dnešní době je celá řada evidencí propojených společným systémem a oddělit tak osobní údaje zaměstnance a vojáka z povolání v určité věcné agendě není možné ani žádoucí.

Nejvíce povinností plynoucích z Obecného nařízení 2016/679 připadá na dílčí správce MO, jakožto přímo podřízené ministrovi obrany (viz obrázek 6). Jedná se o gestory jednotlivých oblastí jednajících za správce, jejichž stěžejním úkolem plynoucím z Obecného nařízení 2016/679 je stanovení účelu a právního základu zpracování osobních údaj a posouzení rizik, které subjektům údajů ze zpracování hrozí. Následným krokem je stanovení organizačních a technických opatření zabezpečujících ochranu osobních údajů a jejich pravidelné hodnocení. Výstupem z plnění povinností

¹⁵⁷ Při ukládání dokumentů v digitální podobě, včetně datových zpráv, je zakázáno v označení ukládaného souboru používat osobní údaje s výjimkou osobního čísla. Při označování předmětu dokumentu nebo spisu v elektronickém systému spisové služby nebo při jejich doručování cestou elektronických komunikací se věta první použije obdobně. Stejně je zakázáno zpracování osobních údajů v metadatech dokumentů v digitální podobě. Viz čl. 10 odst. 1 RMO č. 22/2018.

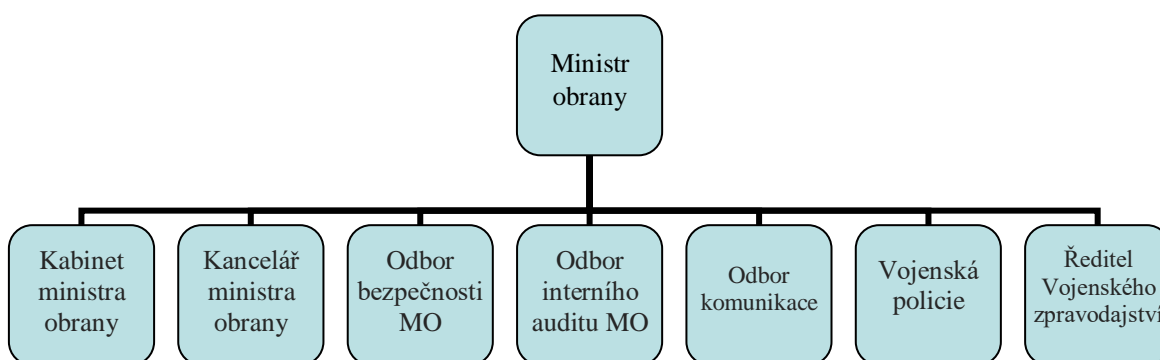
¹⁵⁸ Nelze blíže specifikovat, jelikož se jedná o informace stupně utajení VYHRAZENÉ.

¹⁵⁹ Dle článku 2 odst. 2 písm. a) Obecného nařízení 2016/679.

dílčích správců bude zpracování Zprávy o posouzení vlivu na ochranu osobních údajů a Záznamů o činnostech zpracování pro dílčí evidenci, které následně předkládá pověřenci pro ochranu osobních údajů.

Pro pověřence bude výstupem ze zpracovaných dokumentů zmapování problematiky v celém rezortu MO a také obraz o povědomí jednotlivých vedoucích organizačních celků. Jejich úkolem totiž bude zpracování závěrů z výše uvedených dokumentů do svých organizačních nařízeních, v případě 41. mpr se jedná o již zmíněnou Směrnici k zajištění ochrany osobních údajů. Bude-li některý velitel organizačního celku vyžadovat zpracování osobních údajů, které není v souladu se zákonem, povinnost zpracovat Záznam o činnosti zpracování osobních údajů a Zprávy o posouzení vlivu na ochranu osobních údajů bude čistě v jeho režii a to i přesto, že není dílčím správcem.

Obrázek 6 Schéma přímo podřízených ministrovi obrany



Zdroj: vlastní zpracování

Tak jak plyne z hierarchie nadřízenosti a podřízenosti v rezortu MO, velitelé organizačních celků jsou dále povinni udržovat povědomí svých podřízených ohledně problematiky zpracování osobních údajů a striktně vyžadovat dodržování nastavených zásad.

4.3 Zpracování osobních údajů před a po nabytí účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679 u 41. mpr

4.3.1 Úvodem

Následující podkapitoly budou zaměřeny na jednotlivé druhy fyzických osob v AČR, konkrétně u 41. mpr, na zpracování jejich osobních údajů a dále na komparaci činnosti zpracování osobních údajů před a po nabytí účinnosti Obecného nařízení 2016/679. Metodou řízených rozhovorů bude prozkoumáno povědomí stěžejních pracovníků vybraného útvaru v oblasti zpracování osobních údajů, jejich názory na aplikaci nové právní úpravy a zmíněny poznatky z jejich praxe.

U vojenského útvaru v Žatci jsou zpracovávány osobní údaje u následujících fyzických osob:

- vojáci z povolání (dále jen „VzP“)¹⁶⁰;
- občanskí zaměstnanci (dále jen „o.z.“);
- vojáci v záloze zařazení do aktivní služby (dále jen „AZ“).

Rozdíl mezi jednotlivými kategoriemi spočívá především v rozsahu zpracovávaných osobních údajů a dále v legislativě, ze které dané zpracování vyplývá, viz následující tabulka.

Tabulka 11 Zpracovávané osobní údaje fyzických osob v jednotlivých fázích poměru

Fyzická osoba	Fáze služebního ¹⁶¹ /pracovního poměru				Příslušná legislativa
	Vznik	Průběh	Změny	Zánik	
VzP		x	x	x	Zákon č. 221/1999 Sb., o vojácích z povolání
o.z.	x	x	x	x	Zákon č. 262/2006 Sb., zákoník práce
AZ		x			Zákon č. 45/2016 Sb., o službě vojáků v záloze

Zdroj: vlastní zpracování

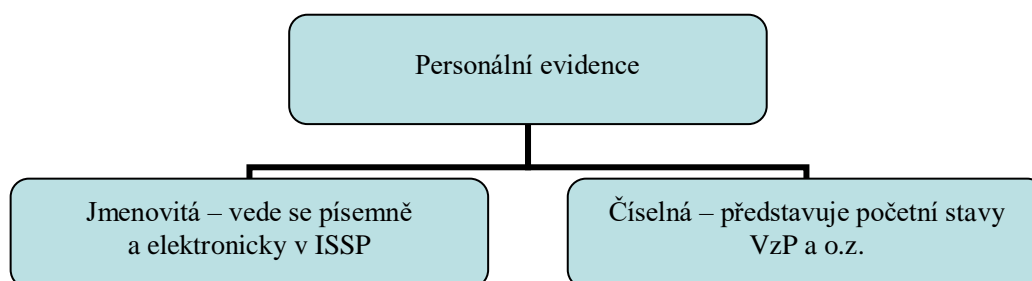
¹⁶⁰ § 2 odst. 1 zákona č. 221/1999 Sb. *Vojákem z povolání je občan, který vojenskou činnou službu vykonává jako svoje zaměstnání. Voják je ve služebním poměru k České republice. Občan může být povolán do služebního poměru jen na základě vlastní žádosti.*

¹⁶¹ § 5 odst. 1 zákona č. 221/1999 Sb. *Služební poměr se zakládá dnem bezprostředně následujícím po dni doručení rozhodnutí služebního orgánu o povolání občana do služebního poměru.*

Zatímco u občanských zaměstnanců se jedná o zpracování osobních údajů napříč všemi fázemi jejich pracovního poměru, u VzP zpracování začíná až na základě služebního zařazení vojáka k vybranému útvaru. Zcela atypická je kategorie AZ, kdy je zpracování údajů při vzniku i zániku služebního poměru v kompetenci Krajského vojenského velitelství, útvar poté řeší pouze průběh jeho služby.

K zabezpečení jednotného postupu při zpracovávání osobních údajů a jako podklad pro personální práci slouží personální evidence fyzických osob¹⁶², která se dle čl. 1 odst. 4 RMO č. 114/2014 dělí na jmenovitou a číselnou (viz obrázek 7).

Obrázek 7 Základní rozdělení personální evidence



Zdroj: vlastní zpracování

Jako základ personální evidence lze považovat jmenovitou evidenci, z které následně vychází evidence číselná.¹⁶³ Pro snadnější orientaci mezi jednotlivými druhy evidencí je v Příloze B znázorněna tabulka se stručným popisem jednotlivých agend.

Jelikož se v číselné evidenci rozeznávají pouze tabulkové a skutečné počty, je její rozdělení podstatně jednodušší. Tabulkovými počty se rozumí počty služebních míst pro fyzické osoby stanovené v tabulce počtů jednotlivých organizačních celků MO a skutečné počty jsou součty fyzických osob u útvaru služebně zařazených, k útvaru přeložených či určených do dispozice velitele organizačního celku.¹⁶⁴ Číselná evidence zahrnuje pomůcky uvedené v následující tabulce.

¹⁶² Článek 1 odst. 1 RMO 114/2014 *Personální evidence je podkladem pro personální práci s vojáky a zaměstnanci a slouží k plnění povinností stanovených právními předpisy.*

¹⁶³ Viz čl. 2 odst. 4 RMO114/2014 *Číselná evidence vychází z evidence jmenovité, tj. z evidenčních pomůcek (např. knihy systemizovaných míst) a z personální dokumentace (např. personálních rozkazů a výnosů ve věcech personálních příslušných služebních orgánů).*

¹⁶⁴ Viz čl. 2 odst. 7 RMO114/2014.

Tabulka 12 Číselná evidence

Název pomůcky	Popis
Početní přehled o obsazenosti tabulkových míst	<ul style="list-style-type: none"> - dává základní přehled o obsazenosti systemizovaných míst stanovených tabulkami počtů; - aktualizuje se při každé změně, která má vliv na tabulkové počty, a při každém personálním opatření, které má vliv na skutečné počty; - slouží pro potřeby služebních, personálních a kontrolních orgánů.
Statistická ročenka	<ul style="list-style-type: none"> - odráží výsledky personální práce s fyzickými osobami v dané podřízenosti za stanovené období, zpravidla za kalendářní rok; - obsahuje údaje, které charakterizují složení profesionálního sboru v dané podřízenosti, a změny, ke kterým během roku došlo.

Zdroj: zpracováno dle RMO č. 114/2014 Personální evidence vojáků z povolání občanských zaměstnanců a zaměstnanců ve správních úřadech

4.3.2 Řízené rozhovory

Pro zjištění podrobnějších informací o běžné praxi zpracování osobních údajů u vybraného útvaru byly provedeny čtyři řízené rozhovory. První byl veden s důstojníkem v oblasti personální (dále jen „personalista“), který je na daném služebním místě zařazen již od října roku 2014. Druhý z nich byl veden s odborníkem v oblasti ekonomického zabezpečení (dále jen „ekonom“), který v oboru působí již třináctým rokem. Další rozhovor byl veden se specialistou v oblasti bezpečnosti komunikačních a informačních systémů (dále jen „IT specialista“), která je náplní jeho práce třetím rokem, a v neposlední řadě byl proveden rozhovor s důstojnicí v oblasti ochrany utajovaných informací (dále jen „důstojnice OUI“), která je na daném místě zařazena přes dva roky. Výše uvedené osoby byly vybrány jakožto stěžejní pracovníci v řešené oblasti, kteří jsou schopni vlivem svých dlouholetých zkušeností posoudit vývoj v dané problematice.

Cílem rozhovorů bylo získat informace o:

- zpracovávaných osobních údajích;
- opatřeních k zabezpečení ochrany osobních údajů;
- zásadních změnách v jejich běžné činnosti;
- úrovni znalostí dané problematiky.

Otázky kladené při řízených rozhovorech jsou uvedeny v příloze této práce. Poněvadž se jednalo o polostrukturovaný rozhovor, byly současně pokládány i doplňující otázky usnadňující pochopení řešené problematiky. Získané informace budou zakomponovány do následujících kapitol.

4.3.3 Zpracování osobních údajů před nabytím účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679

4.3.3.1 Zpracování osobních údajů souvisejících s příchodem fyzických osob k útvaru

Bez ohledu na nabytí účinnosti Obecného nařízení 2016/679 byla agenda spojená s příchodem jednotlivých kategorií fyzických osob vždy značně rozdílná. Odůvodněním je fakt, že v případě VzP se vychází ze zákona č. 221/1999 Sb., o vojácích z povolání, u občanských zaměstnanců je stěžejní ustanovení zákona č. 262/2002 Sb., zákoník práce a zpracování osobních údajů u AZ stanovuje zákon č. 45/2016 Sb., o službě vojáků v záloze. Tabulka 13 představuje přehled zákonných ustanovení ohledně zpracovávání osobních údajů u jednotlivých kategorií osob.

Zatímco u VzP a AZ je výčet zpracovávaných osobních údajů jasně definován, u občanských zaměstnanců se legislativa spokojila s povolením nezbytného minima. Pokud je tedy v zájmu zaměstnavatele zpracovávat i jiné osobní údaje, je nutné mít od o.z. výslovný souhlas obsahující informaci, pro jaký účel zpracování a k jakým osobním údajům se souhlas vztahuje, jakému správci se uděluje a na jaké období. Bartík a Janečková k tomu uvádí, že „*ani na základě souhlasu však nelze (...) zpracovávat osobní údaje absolutně vyňaté z diskrece zaměstnavatele (...)*“¹⁶⁵ Výše uvedené konkretizuje § 12 odst. 2 zákona č. 435/2004 Sb. „*zaměstnavatel nesmí při výběru zaměstnanců vyžadovat informace týkající se národnosti, rasového nebo etnického původu, politických postojů, členství v odborových organizacích, náboženství, filozofického přesvědčení, sexuální orientace, není-li jejich vyžadování v souladu se zvláštním právním předpisem,*¹⁶⁶ *dále informace, které odporují dobrým mravům, a osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem.*“¹⁶⁷

¹⁶⁵ BARTÍK, V., JANEČKOVÁ, E. *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 2016, s. 147.

¹⁶⁶ Zákon č. 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací a o změně některých zákonů (antidiskriminační zákon).

¹⁶⁷ § 12 odst. 2 zákona č. 435/2004 Sb., zákon o zaměstnanosti.

Tabulka 13 Zákonné oprávnění ke zpracovávání osobních údajů u jednotlivých kategorií fyzických osob

Voják z povolání	
§ 2a odst. 1 zákona č. 221/1999 Sb.	Od vzniku služebního poměru do jeho zániku zpracovávají služební orgány tyto osobní údaje vojáka: a) jméno a příjmení, včetně předchozích jmen a příjmení a rodného příjmení, b) akademické tituly a vědecké hodnosti s daty jejich přiznání, c) rodné číslo, d) adresu místa trvalého pobytu a bydliště, e) státní občanství, f) získané vzdělání, g) zdravotní způsobilost k vojenské činné službě h) přehled o předchozích pracovních a služebních poměrech a o samostatných výdělečných činnostech, i) jazykové znalosti a zkoušky z nich, j) zvláštní schopnosti, dovednosti, zájmy a oprávnění, k) trestní bezúhonnost, l) rodinný stav, m) jména, příjmení a adresy místa trvalého pobytu a bydliště osob blízkých.
§ 2a odst. 2 zákona č. 221/1999 Sb.	K doložení údajů podle odstavce 1 je voják povinen předložit platné doklady a podklady. Údaj o trestní bezúhonnosti se prokazuje výpisem z evidence Rejstříku trestů ne starším než 6 měsíců.
§ 2a odst. 3 zákona č. 221/1999 Sb.	Služební orgány vedou osobní údaje v osobním spisu vojáka a zakládají do něj doklady a podklady, které prokazují pravdivost a přesnost osobních údajů. Dále vedou v osobním spisu vojáka doklady a podklady o průběhu jeho služebního poměru. Osobní údaje jsou vedeny i s využitím výpočetní techniky.
Občanský zaměstnanec	
§ 312 odst. 1 zákona č. 262/2006 Sb.	Zaměstnavatel je oprávněn vést osobní spis zaměstnance. Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3 ¹⁶⁸ .
Voják v záloze zařazený do aktivní služby	
§ 3 odst. 1 zákona č. 45/2016 Sb.	O vojácích v záloze se vedou údaje v registru vojáků v záloze, který je samostatnou funkční součástí vojenské evidence podle branného zákona, a to v rozsahu údajů vedených v registru výkonu branné povinnosti a údajů stanovených tímto zákonem.
§ 3 odst. 2 zákona č. 45/2016 Sb.	V registru vojáků v záloze ve službě jsou o vojácích v záloze ve službě vedeny údaje v rozsahu údajů vedených o vzniku a zániku služebního poměru vojáka z povolání podle zákona o vojácích z povolání. ¹⁶⁹

Zdroj: vlastní zpracování

Před nabytím účinnosti Obecného nařízení 2016/679 byl na základě výše uvedeného při vzniku pracovního poměru občanských zaměstnanců vyžadován souhlas, týkající se zpracování osobních údajů zaměstnavatelem, souhlas s pořízením fotografie a hlášením případných změn (viz příloha E). Dalším nezbytným dokumentem v souvislosti

¹⁶⁸ § 3 zákona č. 262/2006 Sb., zákoník práce. „Závislá práce může být vykonávána výlučně v základním pracovněprávním vztahu, není-li upravena zvláštními právními předpisy. Základními pracovněprávními vztahy jsou pracovní poměr a právní vztahy založené dohodami o pracích konaných mimo pracovní poměr.“

¹⁶⁹ § 2a zákona č. 221/1999 Sb., o vojácích z povolání, ve znění pozdějších předpisů.

se zpracováním osobních údajů u o.z. byl souhlas s využitím kontaktních údajů v mimopracovní době (viz příloha F).

Jak již bylo uvedeno, k provádění personální práce s fyzickými osobami v AČR a k zakládání veškeré personální dokumentace slouží osobní spis, jehož členění je znázorněno na obrázku 8. Jedná se o dokumentaci, která je zakládána společně se vznikem služebního/pracovního poměru všech osob, postup je však u jednotlivých kategorií odlišný.

Bez ohledu na nabytí účinnosti Obecného nařízení 2016/679 je praxe taková, že osobní spisy uchazečů o povolání do služebního poměru, tzn. potenciálních VzP, jsou zakládány již na rekručních střediscích¹⁷⁰, a to vždy v jednom výtisku a v listinné podobě. Před samotným zařazením uchazeče do služebního poměru je osobní spis odeslán tomu organizačnímu celku, ke kterému má být voják služebně zařazen.

Proces zpracovávání osobního spisu o.z. je obdobný jako u VzP s tím rozdílem, že jejich osobní spis je zakládán personálním orgánem až u organizačního celku. Zcela odlišný postup je ovšem zaveden u AZ, jejichž spisy jsou založeny příslušným Krajským vojenským velitelstvím¹⁷¹, kde tyto i po celou dobu jejich služebního zařazení zůstávají. Personální orgány příslušného útvaru mají pouze umožněn náhled na osobní spis AZ v Integrovaném subsystému o službě a personálu (dále jen „ISSP“), ale nemají žádnou možnost údaje jakkoliv měnit či doplňovat.

U všech kategorií osob bylo při vzniku služebního/pracovního poměru dále vyžadováno pořízení fotografie¹⁷² a doložení výpisu z Rejstříku trestů¹⁷³.

¹⁷⁰ Rekrutačním střediskem musí projít každý zájemce o uplatnění v ozbrojených silách ČR, studium na vojenských školách nebo informace k zařazení do jednotky aktivní zálohy. Počet rekrutačních středisek se stále navyšuje, aktuální počet je 10 (Praha, Pardubice, České Budějovice, Plzeň, Liberec, Ústí nad Labem, Brno, Olomouc, Ostrava a Jihlava).

¹⁷¹ Krajská vojenská velitelství (dále jen „KVV“) jsou vojenským správním úřadem vykonávajícím ve svém územním obvodu státní správu a současně plní úkoly obrany státu podle zvláštních právních předpisů, zejména zákona č. 585/2004 Sb., o branné povinnosti a jejím zajišťování (branný zákon). V současné době existuje 14 KVV a to KVV hlavní město Praha, Praha Středočeský kraj, Karlovy Vary, Ústí nad Labem, Liberec, Hradec Králové, Pardubice, Jihlava, České Budějovice, Plzeň, Brno, Olomouc, Ostrava a Zlín.

¹⁷² Fotografie je součástí jak osobního spisu, tak je nutným podkladem pro vytvoření Služebního průkazu či jednotného Průkazu MO ke vstupu do objektů.

¹⁷³ Prokázání bezúhonnosti fyzické osoby je nutným požadavkem z hlediska udělení bezpečnostní prověrky pro přístup k utajovaným informacím. Každý příslušník MO musí být držitelem minimálně bezpečnostní prověrky stupně utajení „Vyhrazené“.

Obrázek 8 Členění osobního spisu



Zdroj: vlastní zpracování¹⁷⁴

4.3.3.2 Zpracování osobních údajů souvisejících s průběhem služebního/pracovního poměru fyzických osob

Za nejobsáhlejší agendu personálních orgánů, ať už před nabytím účinnosti Obecného nařízení 2016/679 či nyní, lze bezesporu považovat práci související s průběhem služebního/pracovního poměru fyzických osob. Jakoukoliv změnu služebního/pracovního zařazení nelze realizovat bez podnětu k personálnímu opatření a personálního rozkazu.

Mezi dokumenty zpracovávané v průběhu služby fyzických osob pravidelně, a to 1x ročně, patří služební hodnocení. Jedná se o dokument, který kromě vyhodnocení požadovaných úkolů předchozího roku dále obsahuje osobní údaje fyzických osob, jejich charakteristiku, silné a slabé stránky, informace o vzdělání, zdravotním stavu apod. Jedná se o dokument, který zpracovává přímý nadřízený dané osoby a poté je ukládán do osobního spisu.

Dojde - li v průběhu pracovního/služebního poměru fyzické osoby k rozšíření vzdělání či k absolvování odborného nebo kariérového kurzu, jsou jednotlivci povinni danou skutečnost prokázat. Úkolem personálních orgánů bylo příslušné dokumenty zkontrolovat, ověřené kopie založit do osobního spisu a informaci dále zanést elektronicky

¹⁷⁴ Personální opatření obsahují nejdůležitější osobní data a dávají přehled o občanské i vojenské činnosti fyzických osob.

do ISSP. Uvedeným postupem nedošlo k porušení § 312 odst. 1 zákoníku práce¹⁷⁵ definujícím obsah osobního spisu, jelikož se může jednat o případnou kontrolu splnění podmínek kvalifikace fyzických osob nebo oprávněné zájmy zaměstnavatele. Personalista vybraného útvaru dodává, že „došlo-li k např. k předložení nového občanského průkazu či rodného listu dítěte pro potřeby uplatnění daňového zvýhodnění, léta bylo běžnou praxí automatické pořízení kopie dokumentu a její založení do osobního spisu.“¹⁷⁶

4.3.3.3 Zpracování osobních údajů souvisejících s odchodem fyzických osob od útvaru

Odchodem fyzických osob od útvaru se rozumí nejen převelení k jiným složkám AČR, ale také zánik služebního/pracovního poměru popř. vyhovění žádosti o propuštění z poměru.¹⁷⁷ Mezi dokumenty vyžadující zpracování osobních údajů dále spadá Potvrzení o délce výkonu vojenské činné služby¹⁷⁸ a Určovací lístek sloužící jako doklad při přeložení, odvelení či zániku služebního/pracovního poměru. Odchází-li fyzická osoba do zálohy, je nezbytným dokumentem písemné hodnocení, které se ukládá do osobního spisu jednotlivce.

Při přeložení osob k jinému organizačnímu celku dochází ihned k odeslání osobního spisu k této součásti, při propuštění či zániku poměru se osobní spis odesílá příslušnému Krajskému vojenskému velitelství.¹⁷⁹ V žádném případě není možné osobní spis skartovat.

Šetřením u vybraného útvaru bylo zjištěno, že před nabytím účinnosti Obecného nařízení 2016/679 byl spatřován rozdíl opět u kategorie občanských zaměstnanců, u nichž byl při odchodu vyžadován souhlas ohledně zpracování osobních údajů i po skončení pracovního poměru, a to v rozsahu nezbytném k vypořádání vzájemných práv a povinností a k archivaci osobních údajů (viz příloha G).

¹⁷⁵ Zaměstnavatel je oprávněn vést osobní spis zaměstnance. Osobní spis smí obsahovat jen písemnosti, které jsou nezbytné pro výkon práce v základním pracovněprávním vztahu uvedeném v § 3. Viz § 312 odst. 1 zákona č. 262/2006 Sb., zákoník práce.

¹⁷⁶ Rozhovor s personalistou vybraného útvaru, 10. 7. 2019.

¹⁷⁷ Zánikem služebního/pracovního poměru se rozumí odchod fyzické osoby do zálohy na základě uplynutí sjednaného služebního/pracovního závazku (nedošlo k jeho prodloužení). K propuštění ze služebního poměru dochází na základě žádosti jednotlivé fyzické osoby, kdy je služební/pracovní poměr rozváznán ještě před uplynutím sjednaného závazku.

¹⁷⁸ Dle § 23 zákona č. 221/1999 Sb., o vojácích z povolání, ve znění pozdějších předpisů.

¹⁷⁹ Příslušným Krajským vojenským velitelstvím se rozumí to, v jehož teritoriu nahlásila fyzická osoba trvalý pobyt. Obdobně se postupuje i v případě odnětí vojenské hodnosti či uložení trestu ztráty vojenské hodnosti soudem.

Personalista ke zpracovávání osobních údajů souvisejících s odchodem fyzických osob od útvaru dodává „před GDPR nebyla práva v ISSP¹⁸⁰ správně nastavena, po zániku či propuštění jednotlivce bylo stále možné na osobu v systému nahlížet, a to i v řádu několika let nazpět.“¹⁸¹

4.3.3.4 Shrnutí

Šetřením u vybraného organizačního celku bylo zjištěno, že pro personální orgány je časově i administrativně nejnáročnějším zpracovávání osobních údajů spadajících do fáze průběhu služebního/pracovního poměru fyzických osob a vzhledem k jednotlivým kategoriím osob spadá nejvíce agendy na občanské zaměstnance (blíže kapitola 4.3.3.2). Tuto skutečnost potvrzuje tabulka 14 (Přehled personální evidence u jednotlivých kategorií fyzických osob) obsahující výčet personální evidence v souvislosti s fázemi služebního/pracovního poměru, ve kterých je zpracována.

Kromě agendy plynoucí z RMO č. 114/2014 byly dále personální orgány před nabytím účinnosti Obecného nařízení 2016/679 povinny vyžadovat písemné souhlasy občanských zaměstnanců ohledně zpracování osobních údajů, a to ve všech fázích pracovního poměru.

¹⁸⁰ Systém ISSP by měl správně umožňovat zpracování popř. nahlížení na osobní údaje pouze těch fyzických osob, které jsou zařazeny k danému organizačnímu celku. Na základě odchodu fyzické osoby od útvaru by měl být přístup automaticky odepřen.

¹⁸¹ Rozhovor s personalistou vybraného útvaru, 10. 7. 2019.

Tabulka 14 Přehled personální evidence u jednotlivých kategorií fyzických osob

Název personální evidence	Vznik			Průběh			Zánik		
	VzP	o.z.	AZ	VzP	o.z.	AZ	VzP	o.z.	AZ
Osobní spis		x							
Pomocný osobní spis		x							
Výkaz dob ¹⁸²	x								
Vojenský průkaz	x								
Osobní známka	x	x							
Rozhodnutí služ. orgánu	x	x		x	x		x	x	
Personální rozkaz	x	x		x	x		x	x	
Výnos služ. orgánu ve věcech personálních	x	x		x	x		x	x	
Podnět k PO ¹⁸³	x	x		x	x		x	x	
Oznámení osobní změny				x	x				
Osobní dotazník a životopis		x							
Potvrzení o délce výkonu vojenské činné služby							x		
Určovací lístek				x			x		
Záznam o pohovoru				x	x	x			
Dohoda o zvýšení nebo rozšíření vzdělání				x					
Služební hodnocení				x	x				
Písemné hodnocení při zániku poměru							x		
Oznámení o obdržení OFO ¹⁸⁴ vydávané NBÚ				x					
Popis pracovní činnosti zaměstnance	x	x		x	x				
Záznam o pořízení kopie				x	x				
Abecední kniha				x	x	x			
Deník PO				x	x	x			
Kniha přijatých PO				x	x	x			
Kartotéka vojáků vyřazených z evidence							x		x
Kartotéční lístek studujícího vojen. školy				x					
Kniha systemizovaných míst				x	x	x			
Inventární kniha osobních čísel	x	x	x	x	x	x			
Přehled VzP s přerušeným poměrem							x		

Zdroj: vlastní zpracování

Dále bylo u vybraného útvaru zjištěno, že mezi opomenuté oblasti spadá administrativa spojená s kopírováním občanských průkazů osob. Jelikož se jedná o veřejnou listinu, není zavedená praxe správná, naopak zákon č. 328/1999 Sb., o občanských průkazech tuto činnost výslovně zakazuje. Jak uvádí § 15a odst. 2 tohoto

¹⁸² Pro zabezpečení peněžitými dávkami a pro důchodové pojištění.

¹⁸³ PO – personální opatření.

¹⁸⁴ OFO – Osvědčení fyzické osoby.

zákona, „je zakázáno pořizovat jakýmkoliv prostředky kopie občanského průkazu bez prokazatelného souhlasu občana, kterému byl občanský průkaz vydán, pokud zvláštní zákon nebo mezinárodní smlouva, kterou je Česká republika vázána, nestanoví jinak.“¹⁸⁵

4.3.4 Zpracování osobních údajů po nabytí účinnosti Nařízení Evropského parlamentu a Rady (EU) 2016/679

4.3.4.1 Zpracování osobních údajů souvisejících s příchodem fyzických osob k útvaru

Na základě nabytí účinnosti Obecného nařízení 2016/679 došlo u vybraného útvaru k určitým změnám, především v oblasti edukace zaměstnanců zpracovávajících osobní údaje a dále v oblasti administrativy. Na základě čl. 9 odst. 1 RMO č. 22/2018 bylo u vybraného organizačního celku zabezpečeno seznámení zaměstnanců zpracovávajících osobní údaje s povinnostmi stanovenými dílčím správcem, toto bylo stvrzeno podpisem a založeno.

Jak shodně uvádějí všichni čtyři dotazovaní pracovníci útvaru, pomyslná bublina kolem nabytí účinnosti Obecného nařízení 2016/679 na ně dopadla více v soukromé než pracovní sféře. Jak uvádí ekonom, „mediální tlak byl tak silný, že jsem měl obavy z nárůstu objemu práce, ale v závěru byl dopad na moji práci téměř neznatelný.“¹⁸⁶

Jak již bylo zmíněno v kapitole 4.3.3.1 (Zpracování osobních údajů souvisejících s příchodem fyzických osob k útvaru), občanští zaměstnanci měli za povinnost podepsat souhlas ohledně zpracování osobních údajů (viz příloha E). Ruku v ruce s novým právním rámcem dochází v této oblasti k vytvoření nových formulářů, které kromě poučení dále obsahují výčet právních předpisů, v jejichž rozsahu a účelu jsou osobní údaje zpracovávány, dále kontaktní údaje na pověřence pro ochranu osobních údajů a svolení ke zpracování fotografie jednotlivců (viz příloha H). Podpisem uvedeného formuláře zaměstnanci dále stvrzují poučení v souvislosti s novou platnou legislativou, především s čl. 15, 16, 17, 20 a 21 Obecného nařízení 2016/679.¹⁸⁷

¹⁸⁵ §15a odst. 2 zákona č. 328/1999 Sb., o občanských průkazech.

¹⁸⁶ Rozhovor s ekonomem vybraného útvaru, 10. 7. 2019.

¹⁸⁷ Článek 15 - Právo subjektu údajů na přístup k osobním údajům, čl. 16 - Právo na opravu, čl. 17 - Právo na výmaz („právo být zapomenut“), čl. 20 - Právo na přenositelnost údajů, čl. 21 - Právo vznést námitku.

4.3.4.2 Zpracování osobních údajů souvisejících s průběhem služebního/pracovního poměru fyzických osob

Zpracování osobních údajů v průběhu služebního/pracovního poměru, jakožto ve fázi časově a administrativě nejnáročnější, zaznamenalo nabytím účinnosti Obecného nařízení 2016/679 změny především v oblasti personalistiky. Stejně jako ve fázi příchodu občanských zaměstnanců k útvaru došlo i ve fázi průběhu pracovního poměru k vytvoření nových tiskopisů, a to konkrétně na základě čl. 6 Obecného nařízení 2016/679.¹⁸⁸ Jedná se o souhlasné stanovisko umožňující zaměstnavateli zpracování osobních údajů občanských zaměstnanců nad rámec zákonného povolení (viz příloha I).

Další změna byla zaznamenána v oblasti kopírování veřejných listin, konkrétně občanských průkazů, jelikož pořizování celých průkazů by mohlo mít dopady jak na zaměstnavatele, tak i personalistu útvaru. Odpovědnost zaměstnavatele pramení z Obecného nařízení 2016/679 a zákoníku práce, ale nelze opomenout zákon č. 328/1999 Sb., konkrétně § 15a odst. 2 (blíže v kapitole 4.3.3.4). Personalista k výše uvedenému uvádí „na základě pokynů z Metodického dne personálních orgánů používáme při kopírování občanek šablony, čímž dochází k překrytí nepotřebných údajů.“¹⁸⁹

Po nabytí účinnosti Obecného nařízení 2016/679 zaznamenala určité změny i oblast bezpečnosti komunikačních a informačních systémů. IT specialista výše uvedené potvrzuje slovy „po zavedení GDPR se klade větší důraz na princip *NEED TO KNOW*¹⁹⁰ a každá žádost o vstup do zabezpečeného systému¹⁹¹ je posuzována individuálně. Práva jsou nastavována pouze v rozsahu stanoveném dle služebního zařazení jednotlivce.“¹⁹²

Dále IT specialista poukazuje na skutečnost, že se stále častěji setkává s podceňováním tvorby hesel, „lepení štítků s heslem na monitor už se nám podařilo u útvaru vymýtít, ale problémem poslední doby je používání osobních údajů v heslech do různých systémů. Dojde-li k prozrazení osobních údajů, nepovolaná osoba je následně

¹⁸⁸ Článek 6 odst. 1 písm. a) Obecného nařízení 2016/679 *Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:*

a) subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů.

¹⁸⁹ Rozhovor s personalistou vybraného útvaru, 10. 7. 2019.

¹⁹⁰ V souladu se zásadou *NEED TO KNOW* („potřeba vědět“) by měl být přístup k informacím a jejich držení omezen v rámci určených příslušných orgánů na ty osoby, které z důvodu své pracovní náplně nebo povinností musí být s těmito informacemi obeznámeny nebo s nimi musí zacházet.

¹⁹¹ U vybraného útvaru je zavedeno několik informačních systémů – ŠIS (štábní informační systém), FIS (finanční informační systém), ISSP (integrováný subsystém o službě a personálu, ISL (informační systém logistiky), ESSS (elektronický systém spisové služby), OTS (operačně taktický systém) apod.

¹⁹² Rozhovor s IT specialistou vybraného útvaru, 10. 7. 2019.

schopna rozheslovat přístup do jakkoliv chráněného systému. ¹⁹³ Jak znázorňuje následující tabulka, nejedná se pouze o nešvar vybraného útvaru, nýbrž celorepublikový.

Tabulka 15 Nejčastěji používaná hesla v ČR

P.č.	Heslo	Běžnost v %	P.č.	Heslo	Běžnost v %
1.	123456	0,830	20.	password	0,055
2.	heslo	0,335	21.	slunicko	0,055
3.	12345	0,235	22.	tomas	0,055
4.	123456789	0,195	23.	tunning	0,050
5.	martin	0,135	24.	nevim	0,050
6.	aaaaaa	0,115	25.	killer	0,050
7.	micHAL	0,110	26.	lopata	0,050
8.	internet	0,100	27.	pavel	0,045
9.	666666	0,085	28.	monika	0,045
10.	159753	0,085	29.	lukasek	0,045
11.	hesloheslo	0,080	30.	qwerty	0,045
12.	111111	0,080	31.	poklop	0,045
13.	heslo123	0,065	32.	11111	0,045
14.	genius	0,065	33.	asdfgh	0,045
15.	matrix	0,060	34.	asdasd	0,045
16.	hovno	0,060	35.	nasrat	0,040
17.	12345678	0,060	36.	qwerty	0,040
18.	000000	0,060	37.	jahoda	0,040
19.	ahojky	0,060	38.	lucinka	0,040

Zdroj: zpracováno dle JECAS.CZ. *Jaká hesla často používají čeští uživatelé* [online]. [cit. 2019-07-11]. Dostupný z <https://jecas.cz/nejcastejsi-hesla>.

IT specialista dále uvádí „za největší riziko dnešní doby ale považují sociální sítě. Pomocí osobních údajů jsou vojáci snadno identifikovatelní a tím ohrožují nejen sebe, ale i své rodiny a kolegy.“¹⁹⁴

I přesto, že snahou Evropské unie je stanovení pravidel především k ochraně subjektu údajů, v dnešní pokrokové době mohou být největším nepřítelem subjekty sami sobě. Sociální sítě typu Facebook¹⁹⁵, Instagram¹⁹⁶ či Twitter¹⁹⁷ využívá stále více lidí a často nedomýšlí, jaké dopady může mít jejich zveřejňování či sdílení soukromých

¹⁹³ Rozhovor s IT specialistou vybraného útvaru, 10. 7. 2019.

¹⁹⁴ Rozhovor s IT specialistou vybraného útvaru, 10. 7. 2019.

¹⁹⁵ Facebook je rozsáhlý společenský webový systém sloužící hlavně k tvorbě sociálních sítí, komunikaci mezi uživateli, sdílení multimediálních dat, udržování vztahů a zábavě. Byl založen 1. 2. 2004 a nyní je plně přeložen do osmdesáti čtyř jazyků. Jméno serveru vzniklo z papírových letáků zvaných Facebooks, které se používají na amerických univerzitách a slouží k bližšímu seznámení studentů mezi sebou

¹⁹⁶ Instagram je sociální síť ve formě volně dostupné aplikace pro různé mobilní operační systémy. Svým uživatelům umožňuje sdílení fotografií a videí.

¹⁹⁷ Twitter je poskytovatel sociální sítě a mikrologu, který umožňuje uživatelům posílat a číst příspěvky zasláné jinými uživateli, známé jako tweety.

informací. Pro představu, následující obrázek znázorňuje rozsáhlost pokrytí sociální sítě Facebook po celém světě.

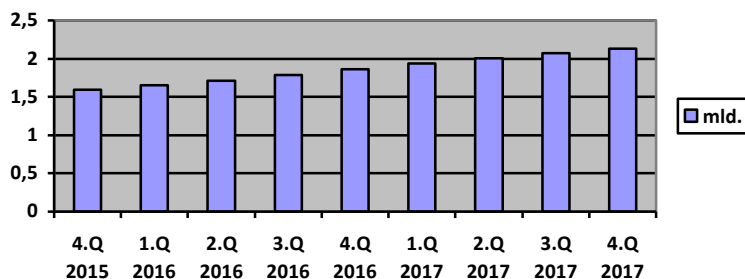
Obrázek 9 Rozsáhlost pokrytí sociální sítě Facebook



Zdroj: CNEWS.CZ, Zprávy. *Facebook má 2,1 miliardy uživatelů. Z každého má korunu denně.* [online]. [cit. 2018-09-29]. Dostupný z <https://www.cnews.cz/facebook-vysledky-q4-2017>

Jak uvádí článek CNEWS.CZ k sociální síti Facebook, jakožto největší sociální síti světa, se celosvětově přihlásí 2,1 miliardy uživatelů alespoň jednou za měsíc, denně pak 1,4 miliardy uživatelů.¹⁹⁸ Nárůst aktivních uživatelů této sociální sítě v období od konce roku 2015 do konce roku 2017 uvádí následující graf.

Graf 1 Nárůst uživatelů sociální sítě Facebook



Zdroj: zpracováno dle CNEWS.CZ, Zprávy. *Facebook má 2,1 miliardy uživatelů. Z každého má korunu denně* [online]. [cit. 2018-09-29]. Dostupný z <https://www.cnews.cz/facebook-vysledky-q4-2017>

¹⁹⁸ CNEWS.CZ, Zprávy. *Facebook má 2,1 miliardy uživatelů. Z každého má korunu denně.* [online]. [cit. 2018-09-29]. Dostupný z <https://www.cnews.cz/facebook-vysledky-q4-2017>.

Je tedy logické, že vlivem nárůstu uživatelů sociálních sítí po celém světě přímou úměrou dochází i k nárůstu uživatelů v podobě fyzických osob sloužících u vybraného útvaru.

4.3.4.3 Zpracování osobních údajů souvisejících s odchodem fyzických osob od útvaru

Při odchodu fyzické osoby od útvaru dochází ruku v ruce k odeslání jejího osobního spisu. V případě přeložení osob je spis ihned odeslán příslušnému organizačnímu celku, je-li osoba propuštěna ze služebního/pracovního poměru, je osobní spis adresován příslušnému krajskému vojenskému velitelství.¹⁹⁹ Společně s osobním spisem lze odeslat i jinou personální evidenci např. Záznamy o odměnách a trestech. Mezi osobní údaje neodmyslitelně patří i zdravotní dokumentace, která je v souvislosti s odchodem fyzických osob odesílána příslušným vojenským poskytovatelům zdravotních služeb. Po uplynutí doby stanovené pro její uložení je dále předána k uložení do Správního archivu AČR.

Zcela nově řešenou oblastí po nabytí účinnosti Obecného nařízení 2016/679 byly fotografie. Pořizování portrétních fotografií fyzických osob v AČR je realizováno na základě právní povinnosti, a sice z důvodu povinnosti prokazovat se služebním průkazem. Polemizovat ale lze nad fotografiemi tzv. reportážními z různých akcí a večírků. Z hlediska Obecného nařízení 2016/679 však není nutné snímky mazat, ale je třeba zohlednit ustanovení občanského zákoníku, konkrétně § 84 a násled.²⁰⁰

Specifikem v oblasti odchodu fyzických osob od útvaru je opět kategorie občanských zaměstnanců, neboť v jejich případě dochází k poučení v souladu s čl. 5 Obecného nařízení 2016/679.²⁰¹ Zaměstnanci jsou dále seznámeni s výčtem osobních údajů, které budou dále zpracovávány za účelem zabezpečení jednotného postupu při realizaci péče o vojenské důchodce prostřednictvím Oddělení péče o vojenské důchodce (viz příloha J).

K nápravě po nabytí účinnosti Obecného nařízení 2016/679 došlo i v oblasti ISSP, kdy bylo zamezeno nahlížení do elektronických osobních spisů osob, které od útvaru v minulosti odešly. Nově je systém nastaven tak, že přístup je automaticky odepřen dnem následujícím po odchodu osoby od daného útvaru.

¹⁹⁹ Obdobně se postupuje i v případě odnětí vojenské hodnosti, ztráty vojenské hodnosti soudem, při úmrtí popř. prohlášení vojáka za mrtvého.

²⁰⁰ Pododdíl 2 Podoba a soukromí (tzn. § 84 – § 90) zákona č. 89/2012 Sb., občanský zákoník.

²⁰¹ Článek 5 Obecného nařízení 2016/679 - Zásady zpracování osobních údajů.

4.3.4.4 Shrnutí

Na základě provedených rozhovorů a šetření u vybraného útvaru bylo zjištěno, že aplikace Evropské právní úpravy v oblasti zpracování osobních údajů přinesla nejednu změnu, především v oblasti administrativy. Nejvíce změn bylo zaznamenáno u kategorie občanských zaměstnanců, neboť zpracovávání jejich osobních údajů vyplývá z jiného právního pověření než u vojáků z povolání a vojáků v záloze zařazených do aktivní služby (blíže kapitola 4.3.1). Aplikace Obecného nařízení 2016/679 s sebou přinesla nutnost vytvořit nové tiskopisy zohledňující novou právní úpravu a větší ochranu nejen pro zaměstnance, ale i pro zaměstnavatele jakožto dílčího správce. Souhlas zaměstnance musí splňovat ustanovení čl. 4 odst. 11 Obecného nařízení 2016/679²⁰², který uvádí, že se musí jednat o „*svobodný, konkrétní, informovaný a jednoznačný projev vůle*“.

V souvislosti se vznikem, průběhem a zánikem služebního/pracovního poměru byla nejvíce diskutovatelnou oblastí personální evidence, konkrétně osobní spis a jeho obsah, dále oprávněnost pořizování portrétních fotografií. Jak uvádí kapitola 4.3.4.3 (Zpracování osobních údajů souvisejících s odchodem fyzických osob od útvaru), nemůže být vůli zaměstnavatele jen tak disponovat fotografiemi svých zaměstnanců, popř. jich využívat k jakýmkoliv účelům.²⁰³

Ke změně došlo i v oblasti kopírování občanských průkazu a rodných listů při uplatňování daňového zvýhodnění. Personalisté i pracovníci v oblasti ekonomického zabezpečení si nově vystačí pouze s kopií veřejné listiny přes šablonu, v případě rodných listů je dostačující opis potřebných údajů.

Bez ohledu na jednotlivé fáze služebního/pracovního poměru, „horkým“ tématem u vybraného útvaru dále byla ochrana osobních údajů v souvislosti s užíváním sociálních sítí a internetu. Všichni oslovení respondenti bez ohledu na jejich odbornost či délku praxe se shodli, že tuto oblast chápou v současné době jako nejrizikovější. Ekonom vybraného útvaru dodává „*ne jednotlivci, ale AČR páchá na internetové síti sebevraždu. Edukace by*

²⁰² Článek 4 odst. 11 Obecného nařízení 2016/679 - *Souhlasem subjektu údajů se rozumí jakýkoliv svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením, své svolení ke zpracování svých osobních údajů.*

²⁰³ BARTÍK, V. JANEČKOVÁ, E. Fotografie v osobním spisu zaměstnance z hlediska zákona o ochraně osobních údajů. In PaM 9/2012.

*měla být zaměřena především na zaměstnance, kteří spravují portály typu army.cz apod.*²⁰⁴

Důstojnice v oblasti OUI dodává „*vlivem GDPR je vyvíjen větší tlak na ochranu osobních údajů než dříve, nejde jen o data jako taková, v naší oblasti se může jednat o prozrazení vojenských operací či ohrožení rodinných příslušníků vojáků. V současné době je informovanost v této oblasti nutností.*“²⁰⁵

Jedním z cílů řízených rozhovoru bylo i zjištění, jaká technická a bezpečnostní opatření k ochraně osobních údajů jsou u útvaru používána. Bez ohledu na služební zařazení jednotlivých respondentů jejich odpovědi byly téměř totožné, neboť všichni vycházejí již z ustanovení RMO č. 16/2013²⁰⁶. Důraz je kladen především na organizační požadavky při zpracování osobních údajů (viz Směrnice 41. mpr, blíže v kapitole 4.1.3.3), fyzickou bezpečnost a řízený přístup osob ke zpracovávaným osobním údajům, a to prostřednictvím přístupových práv do informačních systémů jednotlivých oblastí:

- personální – Informační systém o službě a personálu;
- ekonomická – Finanční informační systém;
- komunikačních a informačních systémů – Štábní informační systém;
- ochrany utajovaných informací – Elektronický systém spisové služby.

4.4 Zhodnocení výsledků a doporučení

4.4.1 Zhodnocení výsledků a doporučení ke zpracování osobních údajů v AČR

Pro zabezpečení jednotného postupu při zpracování osobních údajů a jejich ochraně jednotlivými organizačními celky AČR a k zabezpečení plnění povinností, které vyplývají při zpracování těchto údajů z Obecného nařízení 2016/679, byl ministryní obrany dne 23. května 2018 vyhlášen rozkaz č. 22/2018. Tímto došlo k posílení stavebních kamenů, které byly postaveny na základě řádného plnění ustanovení zákona č. 101/2000 Sb. a rozkazu ministra obrany č. 16/2013.

Prostřednictvím RMO č. 22/2018 došlo k dostatečnému ošetření problematiky ochrany osobních údajů včetně nastavení standardů k jejímu zajištění. Jak blíže uvádí

²⁰⁴ Rozhovor s ekonomem vybraného útvaru, 10. 7. 2019.

²⁰⁵ Rozhovor s důstojnicí OUI vybraného útvaru, 10. 7. 2019

²⁰⁶ Hlava II RMO č. 16/2013 Věstníku O ochraně určených neutajovaných informací v rezortu Ministerstva obrany – Opatření k zajištění bezpečnosti určených neutajovaných informací.

kapitola 8.1.5 (Stanovení předběžných organizačních a technických opatření), jedná se především o bezpečnostní politiku při činnosti zpracování, důslednou edukaci zaměstnanců, fyzické zabezpečení či vhodné nastavení organizačních a technických opatření.

V souvislosti s platnou právní úpravou a s ohledem na činnost příslušníků AČR lze při zpracovávání osobních údajů doporučit následující zásady:

- 1) pravidelná aktualizace organizačních nařízení týkajících se ochrany osobních údajů u všech organizačních celků;
- 2) snaha o minimalizaci dat, tzn. vést jednoduchou správu a shromažďovat pouze nezbytně nutná data, včetně nastavení procesů při změně služebního zařazení či zániku služebního poměru;
- 3) pro zaměstnance určené ke zpracovávání osobních údajů zřídit přístupová oprávnění a to dle konkrétních práv, která v souvislosti s osobními údaji jednotlivci mají;
- 4) z hlediska bezpečnostních opatření využívat pseudonymizaci či anonymizaci osobních údajů, zabezpečení či zálohování dat (blíže v kapitole 4.2.1.1 Promítnutí základních pojmů Nařízení Evropského parlamentu a Rady (EU) 2016/679 do problematiky zpracování osobních údajů);
- 5) reagovat na změny bezpečnostní situace a vhodnými opatřeními chránit zvláště příslušníky AČR vyslané do zahraničních operací, včetně jejich nejbližších.

V případě, že vedoucí organizačního celku není schopen sám vyhodnotit situaci a přijmout potřebná opatření, pověřenec pro ochranu osobních údajů je připraven poskytnout metodickou pomoc. Dle pověřence pro ochranu osobních údajů je praxe na Odboru bezpečnosti Ministerstva obrany momentálně taková, že v případě potřeby poskytují metodickou pomoc přímo na vojenském útvaru. Vyžaduje-li to situace, účastní se návštěvy i gestor dané oblasti, a to například z Odboru bezpečnosti či komunikace MO.

4.4.2 Zhodnocení výsledků a doporučení ke zpracování osobních údajů u 41. mpr

Na základě promítnutí Obecného nařízení 2016/679 do problematiky zpracování osobních údajů u 41. mpr byly analyzovány dopady na fyzické osoby a navržena doporučení ke zlepšení ochrany jejich osobních údajů při zpracování.

Šetřením bylo zjištěno, že standardy k zajištění ochrany osobních údajů u 41. mpr jsou vhodně nastaveny a dodržovány. Směrnice 41. mpr, která je vlivem fluktuace lidí jakýmsi „živým“ dokumentem, je prostřednictvím měsíčních doplňků do Organizačního rozkazu průběžně aktualizována.

Uživatelé informačních systémů absolvovali školení se zaměřením na dodržování ustanovení RMO č. 22/2018 především v souvislosti s označováním dokumentů osobními údaji ve svých agendách, které bylo do té doby standardně používáno.

I přesto, že většina příslušníků 41. mpr zaznamenala určité změny v oblasti ochrany osobních údajů, a to především vlivem médií a „bublině“ kolem Obecného nařízení 2016/679, ne všichni si uvědomují, že prioritou jsou právě oni jakožto subjekty údajů. Trefně by se celá situace dala vystihnout citátem spisovatele Arthura Conana Doylea²⁰⁷, a sice že: „*Každý řetěz je silný jen tak, jak je silný jeho nejslabší článek*“. Sebelepší stanovená organizační a technická opatření k ochraně osobních údajů totiž nezaručí, že ke zneužití nedojde právě na základě selhání lidského faktoru.

Prioritou 41. mpr by proto mělo být hlavně zaměření na jednotlivce, na jejich podceňování problematiky nakládání s osobními údaji a na možné důsledky tohoto konání. V rámci školení příslušníků útvaru se nezaměřovat pouze na papírovou či elektronickou evidenci osobních údajů, ale povědomí u jednotlivců směřovat především k rizikům plynoucím z používání internetu a „chytrých“ telefonů, neboť k úniku informací služebního charakteru může dojít nejen z prostoru vojenského objektu, ale i v průběhu osobního volna. Míra toho rizika poté roste v případě, že je příslušník útvaru vyslán k plnění úkolů do zahraničí.

K výše uvedené problematice je v prostředí sítě Internet doporučeno nezveřejňovat:

- fotografie pořízené v průběhu služební činnosti,
- fotografie služebního charakteru,
- vlastní fotografie zachycující vojáka během služební činnosti,
- fotografie zachycující vojáka mimo služební činnost s výstrojnými nebo výzbrojnými součástkami AČR nebo koaličních partnerů,
- fotografie zachycující vojenskou techniku během výcviku nebo nasazení,
- videozáznamy, které zachycují služební činnost,

²⁰⁷ Arthur Conan Doyle (1859 – 1930) - skotský lékař a spisovatel.

- zvukové záznamy služebního charakteru,
- psaný text popisující informace služebního charakteru,
- jakékoliv jiné informace služebního charakteru.

Je nutné zdůraznit dodržování stávajících právních a vnitřních předpisů, zejména:

- zákona č. 221/1999 Sb. „zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděl při výkonu služby a které v zájmu služby nelze sdělovat jiným osobám; to neplatí, pokud byl této povinnosti zproštěn služebním orgánem“²⁰⁸
- zákona č. 234/2014 Sb., „zachovávat mlčenlivost o skutečnostech, o nichž se dověděl při výkonu služby, a které v zájmu služebního úřadu nelze sdělovat jiným osobám; to neplatí, pokud byl této povinnosti zproštěn; povinnost zachovávat mlčenlivost, která státnímu zaměstnanci vyplývá z jiného zákona, není dotčena“²⁰⁹
- zákona č. 262/2006 Sb., „zachovávat mlčenlivost o skutečnostech, o nichž se dozvěděli při výkonu zaměstnání a které v zájmu zaměstnavatele nelze sdělovat jiným osobám; to neplatí, pokud byli této povinnosti zproštěni statutárním orgánem nebo jím pověřeným vedoucím zaměstnancem, nestanoví-li zvláštní právní předpis jinak“²¹⁰.

Společným dodržováním výše uvedených zásad všemi fyzickými osobami dojde k ochraně vojenského útvaru jako celku a s tím související minimalizací možného zneužití jak osobních údajů jednotlivců, tak vyzrazení informací služebního charakteru 41. mpr, potažmo Armády ČR. V případě porušení stanovených opatření je nutné dovést trestněprávní či kázeňskou odpovědnost konkrétních osob a přijmout odpovídající personální opatření.

²⁰⁸ § 48 odst. 1 písm. c) zákona č. 221/1999 Sb., o vojácích z povolání, ve znění pozdějších předpisů.

²⁰⁹ § 77 odst. 1 písm. h) zákona č. 234/2014 Sb., o státní službě, ve znění pozdějších předpisů.

²¹⁰ § 303 odst. 2 písm. b) zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.

5 Výsledky a diskuze

5.1 K vývoji právní úpravy v oblasti ochrany a zpracování osobních údajů

Na základě analýzy historického vývoje právní úpravy v oblasti ochrany a zpracování osobních údajů byly zjištěny hlavní nedostatky předchozích právních úprav. Za první dokument zohledňující výše zmíněnou problematiku lze považovat Všeobecnou deklaraci lidských práv a následně Evropskou úmluvu o ochraně lidských práv a základních svobod. Za společný nedostatek obou právních úprav lze považovat pouze obecné prohlašování práva na soukromí a nedostatečné zohlednění ochrany osobních údajů při jejich zpracování (blíže v kapitole 3.1.1).

V předrevolučním období vchází v platnost prototypový dokument zahrnující nově i zpracování osobních údajů, a to Úmluva Rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat. Dokument sice deklaruje každé fyzické osobě na území každé smluvní strany úctu k jejím právům, základním svobodám a především k jejím právům na soukromý život, ale zahrnuje pouze částečné či plně automatizované zpracování. Kromě výše uvedeného se Úmluva č. 108/1981 potýká s nedostatkem v oblasti právní úpravy sjednocení ochrany osobních dat v evropském prostoru v souvislosti s růstem technologického vývoje (blíže v kapitole 3.1.2).

Snaha o určité sjednocení právní úpravy přichází v porevolučním období v podobě Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. 10. 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Tento dokument již pamatuje na neautomatizované zpracování osobních údajů, ale na základě nepřímých stanovených práv a povinností subjektům vnitrostátního práva nedochází k očekávanému harmonizačnímu účinku (blíže v kapitole 3.1.3).

Snaha České republiky o členství v Evropské unii vedla k přijetí zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů jakožto dokumentů zajišťujících kompatibilitu s předpisy Evropské unie. Tento zákon lze charakterizovat jako klíčový v oblasti ochrany osobních údajů v České republice, neboť vedl k posílení postavení jednotlivce jako subjektu údajů, zaručil ochranu před neoprávněnými zásahy do jeho soukromí a nově rozlišoval automatizované i neautomatizované zpracování osobních údajů (blíže v kapitole 3.1.4).

Za zásadní dopad v souvislosti s přijetím zákona č. 101/2000 Sb. lze spatřovat i stanovení sankcí v případě porušení ochrany osobních údajů, jakožto do té doby zcela opomíjenou oblast, a dále ustanovení kontrolního orgánu k posílení ochrany subjektů údajů (blíže v kapitole 3.3.2).

5.2 K implementaci Obecného nařízení 2016/679 u 41. mpr

Reakce ministerstva obrany na nabytí účinnosti Obecného nařízení 2016/679 přichází v podobě vyhlášení Rozkazu ministryně obrany č. 22/2018 Věstníku o zpracování a ochraně osobních údajů dne 23. května 2018. Jedná se o dokument zabezpečující jednotný postup při zpracování a ochraně osobních údajů a plnění povinností, které plynou z přímo použitelného nařízení Evropské unie (blíže v kapitole 4.2.1).

Důraz je položen především na vysvětlení nově zavedených pojmů a na objasnění povinností dílčích správců či zaměstnanců při zpracovávání osobních údajů. Rozkaz se dále podrobně zabývá novou problematikou posouzení vlivu na ochranu osobních údajů, jež se týká těch vedoucích organizačních celků, kteří zvažují zpracování osobních údajů, které není stanoveno právním předpisem. Jelikož vybraný útvar momentálně zpracovává pouze běžnou, nerizikovou agendu, je tato oblast blíže rozpracována v samostatné příloze (viz Příloha A - Posouzení vlivu na ochranu osobních údajů).

I přesto, že dle ustanovení čl. 2 odst. 2 písm. a) se evropské nařízení nevztahuje na zpracování prováděné v rámci výkonu činnosti, která nespadá do oblasti působnosti práva Unie, je snahou rezortu MO jeho aplikace do praxe. Na základě výše uvedeného je hlavním cílem implementace Obecného nařízení 2016/679, potažmo RMO č. 22/2018, aktualizace stěžejních dokumentů 41. mpr, ať už se jedná o Směrnici ke zpracování osobních údajů, Organizační rozkaz, Plán zabezpečení kontinuity či popisy funkčních náplní jednotlivých fyzických osob.

Na základě provedených řízených rozhovorů bylo zjištěno, že oslovení respondenti určité povědomí o nové evropské právní úpravě mají, ale jelikož v rámci svého služebního zařazení vycházejí z ustanovení vnitřních předpisů, nebyli nuceni se blíže s obsahem Obecného nařízení 2016/679 seznamovat. Své znalosti definují jako částečné, přesto nabytí platnosti evropského nařízení hodnotí spíše pozitivně, a to především na základě zkušeností plynoucích ze soukromé sféry (blíže v kapitole 4.3.4).

5.3 K povinnostem zaměstnanců 41. mpr při zpracovávání osobních údajů

Na základě šetření u vybraného útvaru bylo zjištěno, že zaměstnanci praporu, kteří jsou oprávněni v rámci svého služebního/pracovního zařazení zpracovávat osobní údaje, jsou povinni tak učinit pouze v rozsahu, způsobem, prostředky a po dobu, která je stanovena velitelem organizačního celku. Rozsah zpracovávaných údajů představuje přesně definovaný výčet osobních údajů ke stanovenému účelu a je určen pro jednotlivce vojenského útvaru, popř. pro skupiny se shodným popisem pracovní činnosti spojené se zpracováváním osobních údajů (blíže v kapitole 4.1.3.3).

V případě zpracování osobních údajů v listinné podobě je kladen důraz na uložení dokumentace v uzamykatelné místnosti popř. v uzamykatelném úschovném obalu. K elektronickému zpracování osobních údajů jsou využívány informační systémy, do nichž je přístup zabezpečen heslem. Je-li pro zpracování osobních údajů vyžadován písemný souhlas subjektu údajů, odpovídá za jeho zajištění oprávněný zaměstnanec.

Doba uchování osobních údajů je stanovena po dobu trvání služebního/pracovního poměru fyzických osob a po jeho skončení po dobu nezbytně nutnou k vypořádání vzájemných práv a povinností. Skartace dokumentů je řešena v souladu se Spisovým řádem MO²¹¹ (blíže v kapitole 4.2.1.2).

Na základě rostoucí digitalizace napříč všemi odvětvími by se dalo očekávat snížení byrokracie i v rezortu ministerstva obrany, ale opak je pravdou. Systémy (konkrétně ISSP) používané u 41. mpr sice umožňují generování potřebných formulářů a jejich následné vložení do elektronických spisů jednotlivců, ale dosud nejsou zřízeny elektronické podpisy. Výše uvedené v praxi znamená daný formulář vygenerovat, vytisknout, nechat podepsat fyzickou osobou, a pokud chceme mít elektronickou databázi, tak daný formulář naskenovat a poté teprve vložit do systému. Digitalizace by tedy byla ku prospěchu věci, ale zatím je v popředí spíše nárůst byrokracie.

Na základě zjištěného stavu zpracování osobních údajů u 41. mpr lze jako vhodný nástroj navrhnout dodržování stěžejních zásad, ať už se zaměřením na pravidelnou aktualizaci či snahou o minimalizaci dat (blíže v kapitole 4.4.1).

²¹¹ Příloha č. 2 k RMO č. 34/2017 Věstníku Spisový řád Ministerstva obrany.

5.4 K bezpečnostním opatřením při zpracování osobních údajů u 41. mpr

Na základě šetření u 41. mpr, lze bezpečnost osobních údajů při zpracovávání rozdělit na administrativní, personální, fyzickou a v neposlední řadě na bezpečnost komunikačních a informačních systémů.

V oblasti administrativy je položen důraz na označení dokumentů a nosičů obsahujících osobní údaje či pořizování jejich kopií, které je umožněno pouze s vědomím přímého nadřízeného na vyčleněných kopírovacích zařízeních. Personální opatření souvisí především se seznámením fyzických osob se zásadami ochrany osobních údajů nejpozději v den vzniku služebního/pracovního poměru. Fyzické osoby oprávněné zpracovávat osobní údaje musí být seznámeny s rozsahem a podmínkami tohoto zpracování a jejich popis pracovní/služební náplně musí být o toto oprávnění rozšířen.²¹² Nejpozději v den skončení služebního/pracovního poměru je odchozí fyzická osoba poučena o zachování mlčenlivosti o skutečnostech, o nichž se dozvěděla v průběhu pracovního/služebního poměru a které v zájmu zaměstnavatele nelze sdělovat jiným osobám.

V oblasti fyzické bezpečnosti je kladen důraz na uložení osobních údajů v prostorech, které zabezpečí jejich ochranu, a dále na režim vstupu do těchto zabezpečených oblastí. U 41. mpr je zavedena elektronická úschovna klíčů, která dle nastavených oprávnění zabezpečuje režim vstupu jednotlivých osob a zároveň eviduje historii pro případnou kontrolu (blíže v kapitole 4.1.3.3).

Bezpečnost komunikačních a informačních systémů zabezpečuje přístup k osobním údajům pouze osobám s oprávněným přístupem k dané informaci a za dodržení stanovených pravidel. Přístup do informačního systému musí být zabezpečen heslem, které je v pravidelných intervalech aktualizováno. Dále bezpečnost apeluje na zákaz přenášení osobních údajů v otevřené podobě v prostředí internetu a jejich zveřejňování na portálech či sociálních sítích. K výše uvedenému jsou minimálně 1x ročně prováděna školení všech osob, záznamy a absolvování jsou poté uchovávány minimálně pod dobu jednoho roku.

Šetřením bylo zjištěno, že v rezortu ministerstva obrany došlo k nárůstu případů, kdy se v prostředí internetu objevily informace nevhodné pro oči veřejnosti, tzn. informace

²¹² Popis pracovní/služební náplně fyzické osoby oprávněné zpracovávat osobní údaje musí obsahovat následující sdělení: „Jsem oprávněn(a) k přístupu a nakládání s osobními údaji v rozsahu a za podmínek stanovených ve Směrnici k zajištění ochrany osobních údajů.“

služebního charakteru. Na základě výše uvedeného byla v praktické části práce navržena opatření k eliminaci těchto případů (blíže v kapitole 4.4.2).

Jako vhodný nástroj k rozšíření povědomí zaměstnanců 41. mpr o výše uvedené problematice lze využít pravidelná školení v oblasti ochrany utajovaných informací, jejichž absolvování je zakotveno v zákoně č. 412/2005 Sb.²¹³ a týká se všech příslušníků 41. mpr. Dojde-li k jakémukoliv porušení ochrany informací, stávají se podpisy jednotlivců v prezenční listině uchopitelným důkazem o jejich řádném seznámení a porozumění dané problematice a také nástrojem k vedení jednotlivce k odpovědnosti.

5.5 K povinnostem při zjištění případů porušení zabezpečení osobních údajů

V případě porušení zabezpečení osobních údajů je velitel 41. mpr povinen informaci ihned předat pověřenci pro ochranu osobních údajů, v jehož kompetenci je její posouzení. Velitel organizačního celku následně přijímá taková opatření, aby došlo k řádnému prošetření narušení ochrany osobních údajů a ke zhodnocení, zda byla řádně dodržena nastavená bezpečnostní pravidla. Informace zjištěné na základě šetření společně s návrhem na zamezení opakování dané události následně zasílá pověřenci a státnímu tajemníkovi v ministerstvu (blíže v kapitole 4.2.1.5).

Na základě prošetření vzniklé události je dále velitel organizačního celku kompetentní vést fyzickou osobu k odpovědnosti. V případě pochybení u VzP a AZ dochází k aplikaci ustanovení čl. 53 odst. 2 zákona č. 221/1999 Sb.,²¹⁴ v případě občanských zaměstnanců bude stěžejní ustanovení zákoníku práce. U všech kategorií fyzických osob je praxe vojenského útvaru taková, že postačí-li k nápravě osoby a k obnovení služební/pracovní kázně vytknutí méně závažného jednání, k uložení kázeňského trestu v závěru dojít nemusí.

²¹³ *Odpovědná osoba je povinna zajistit jednou ročně provedení proškolení fyzických osob, které mají přístup k utajované informaci, z právních předpisů v oblasti ochrany utajovaných informací a vést o těchto proškoleních přehledy. Viz § 67 odst. 1 písm. b) zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti.*

²¹⁴ *Kázeňskými tresty jsou:*

a) napomenutí,

b) písemná důtka,

c) výstraha pro neodpovědný výkon služby,

d) snížení služebního platu až o 15 % až na dobu 6 měsíců. Viz článek 53 odst. 2 zákona č. 221/1999 Sb., o vojácích z povolání.

Takový přístup k dané problematice není vhodným řešením, neboť je všeobecně známé, že pokud v případě porušení povinností nedojde k řádnému exemplárnímu potrestání, vede situace k podceňování problematiky a k další lehkovážnosti. Jako řešení k výše uvedenému je navrženo striktní dodržování příslušných právních a vnitřních předpisů, především v souvislosti se zachováním mlčenlivosti o informacích „služebního charakteru“ (blíže v kapitole 4.4.2).

6 Závěr

Vlivem technologického pokroku posledních let je rozsah zpracovávaných informací o každém z nás mnohonásobně rozsáhlejší než byl kdokoli schopný v minulosti předvídat. Mnohým se může zdát, že Obecné nařízení 2016/679 je nástroj k legálnímu nakládání s našimi osobními údaji, ale opak je pravdou. Snahou nové evropské úpravy je nastavení takových pravidel a povinností pro zpracovatele osobních údajů, jejichž prioritou je ochrana všech subjektů údajů v celé Evropské unii.

Historicky první dokument zajišťující určitou ochranu jednotlivce, a sice právo na jeho soukromí, vchází v platnost již koncem roku 1948 prostřednictvím Všeobecné deklarace lidských práv. Jednalo se o dokument reagující na danou dobu, ale na základě pokroku v oblasti technologií bylo nutné reagovat vývojem legislativy nové.

Analýza platné právní úpravy ochrany a zpracování osobních údajů v ČR, jakožto jeden z cílů diplomové práce, přináší přehled vývoje ochrany osobních dat u nás. Jako stěžejní lze chápat až zákon č. 101/2000 Sb., který byl vyústěním snahy České republiky o členství v Evropské unii. Jedná se o první právní předpis zajišťující kompatibilitu české právní úpravy s evropskou, který prostřednictvím novelizací pružně reaguje na evropské trendy.

Součástí teoretické části je dále komparace zákona č. 101/2000 Sb. s novým zákonem o zpracování osobních údajů, včetně porovnání vývoje sankcí v případě porušení povinností fyzických či právnických osob. S přijetím Obecného nařízení 2016/679 byla problematika finančních postihů jedna z nejobávanějších oblastí, ale Česká republika možnosti navýšení sankcí téměř nevyužila. Naopak za zásadní lze považovat zcela nová či upravená práva subjektů údajů, změny v oblasti zajištění činnosti a struktury nezávislého dozorového orgánu či zavedení pověřence pro ochranu osobních údajů.

Praktická část se zaměřila na analýzu nové právní úpravy zpracovávání osobních údajů v prostředí Armády České republiky, konkrétně u 41. mechanizovaného praporu v Žatci. Na základě promítnutí Obecného nařízení 2016/679 do problematiky zpracovávání osobních údajů a komparace vnitřních předpisů rezortu Ministerstva obrany byly zjištěny základní principy používané při zpracovávání osobních údajů při vzniku, průběhu či odchodu fyzických osob ze služebního/pracovního poměru. Formou řízených rozhovorů se čtyřmi vedoucími pracovníky byly zjištěny podrobnější informace o běžné praxi zpracovávání osobních údajů u vybraného útvaru, což v závěru vedlo k návrhům

případných změn. Závěrečná část syntetizovala zjištěné poznatky a v souvislosti s platnou právní úpravou a s ohledem na činnost příslušníků AČR navrhla zásady vhodné pro zpracovávání osobních údajů.

Závěry diplomové práce jsou praktickým přínosem nejen pro vybraný vojenský útvar, ale jsou obecně platné pro všechny útvary Armády České republiky. Stěžejním doporučením je zaměření na jednotlivce, neboť i sebelepší ochrana či bezpečnostní systém nedokáže zamezit pochybením způsobeným vlastní vinou. Budou-li subjekty údajů i nadále přistupovat k dané problematice bez nutného respektu, postupem času zjistí, že evropské nařízení je sice průlomové, ale není „všemocné“.

7 Seznam použitých zdrojů

7.1 Prameny mezinárodního a evropského práva

Evropská úmluva o ochraně lidských práv a základních svobod ze dne 4. listopadu 1950

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

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

Směrnice Evropského parlamentu a Rady (EU) 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

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

Úmluvu Rady Evropy č. 108/1981, o ochraně osob se zřetelem na automatizované zpracování osobních dat

Všeobecná deklarace lidských práv ze dne 10. prosince 1948

7.2 Právní předpisy

Usnesení předsednictva České národní rady o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky ve znění zákona 162/1998 Sb.

Ústavní zákon č. 1/1993 Sb., Ústava České Republiky ze dne 16. prosince 1992 ve znění pozdějších ústavních předpisů

Vyhláška č. 98/2012 Sb. o zdravotnické dokumentaci ve znění pozdějších předpisů

Zákona č. 140/1961 Sb., Trestní zákon ve znění pozdějších předpisů

Zákon č. 582/1991 Sb., o organizaci a provádění 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 příjmu ve znění pozdějších předpisů

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

Zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů ve znění pozdějších předpisů

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

Zákon č. 219/1999 Sb., o ozbrojených silách České republiky ve znění pozdějších předpisů

Zákon č. 221/1999 Sb., o vojácích z povolání ve znění pozdějších předpisů

Zákon č. 219/1999 Sb., o ozbrojených silách České republiky ve znění pozdějších předpisů

Zákon č. 328/1999 Sb., o občanských průkazech ve znění pozdějších předpisů

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

Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů ve znění pozdějších předpisů

Zákon č. 435/2004 Sb., zákon o zaměstnanosti ve znění pozdějších předpisů

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) ve znění pozdějších předpisů

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění pozdějších předpisů

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

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

Zákon č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy ve znění pozdějších předpisů

Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách) ve znění pozdějších předpisů

Zákon č. 373/2011 Sb., o specifických zdravotních službách ve znění pozdějších předpisů

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

Zákon č. 46/2016 Sb., o službě vojáků v záloze ve znění pozdějších předpisů

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

7.3 Vnitřní předpisy

Rozkaz ministra obrany č. 16/2013 Věstníku O ochraně určených neujasněných informací v rezortu Ministerstva obrany ve znění pozdějších předpisů

Rozkaz ministra obrany č. 114/2014 Věstníku Personální evidence vojáků z povolání občanských zaměstnanců a zaměstnanců ve správních úřadech ve znění pozdějších předpisů

Rozkaz ministra obrany č. 9/2017 Věstníku Stanovení pořadí vojáků z povolání pro realizaci personálních opatření systému řízení kariér ve znění pozdějších předpisů

Rozkaz ministra obrany č. 34/2017 Věstníku Spisový řád Ministerstva obrany

Rozkaz ministryně obrany č. 22/2018 Věstníku Zpracování a ochrana osobních údajů v rezortu Ministerstva obrany ve znění pozdějších předpisů

Rozkaz ministryně obrany č. 26/2018 Věstníku, kterým se mění rozkaz ministra obrany č. 114/2014 Věstníku, Personální evidence vojáků z povolání a občanských zaměstnanců ve znění pozdějších předpisů

7.4 Tištěná literatura

BARTÍK, Václav, JANEČKOVÁ, Eva. *Fotografie v osobním spisu zaměstnance z hlediska zákona o ochraně osobních údajů*. In PaM 9/2012.

BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi (vybrané problémy)*. 4. vyd. Praha: Wolters Kluwer ČR, a.s., 2016. 290 s. ISBN 978-80-7552-141-5.

BULLA, Miroslav. *Osobní údaje v elektronické podobě a GDPR*. In PaM 5/2018.

JANEČKOVÁ, Eva. *GDPR. Praktická příručka implementace*. 1. vyd. Praha: Wolters Kluwer, 2018. 136 s. ISBN 978-80-7552-248-1.

MATOUŠOVÁ, Miroslava, HEJLÍK, Ladislav. *Osobní údaje a jejich ochrana*. 2. vyd. Praha: ASPI, Wolters Kluwer ČR, a.s., 2008. 468 s. ISBN 978-80-7357-322-5.

NEZMAR, Luděk. *GDPR: Praktický průvodce implementací*. 1. vyd. dotisk. Praha: GRADA Publishing, a.s., 2017. 301 s. ISBN 978-80-271-0668-4.

NULÍČEK, Michal a kol. *GDPR/Obecné nařízení o ochraně osobních údajů (2016/679/EU) – Praktický komentář*. 2. vyd. Praha: Wolters Kluwer ČR, a.s., 2018. 580 s. ISBN 978-80-7598-068-7.

PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě. Komentář*. 1. vyd. Praha: Leges, 2018. 488 s. ISBN 978-80-7502-288-2.

Právní rozhledy: časopis pro všechna právní odvětví. *Vláda schválila návrh zákona o zpracování osobních údajů*. Praha: C.H. Beck/SEVT, 8/2018. ISSN 1210-6410.

ŽŮREK, Jiří. *Praktický průvodce GDPR*. 1. vyd. dotisk. Olomouc: ANAG, 2017. 223 s. ISBN 978-80-7554-097-3.

ŽŮREK, Jiří. *GDPR v personalistice*. 1. vyd. Olomouc: ANAG, 2019. 176 s. ISBN 978-80-7554-210-6.

7.5 Elektronické dokumenty

ARMY.CZ, Armáda České republiky. *Armáda České republiky se představuje* [online]. [cit. 2018-07-11]. Dostupný z: <http://www.acr.army.cz/scripts/detail.php?id=5090>

ARMY.CZ, Armáda České republiky. *Struktura Velitelství pozemních sil AČR* [online]. [cit. 2018-07-11]. Dostupný z: <http://www.acr.army.cz/struktura/generalni-stab/velitelstvi-pozemnich-sil-86865/>

ARMY.CZ, Armáda České republiky. *Struktura Velitelství vzdušných sil AČR* [online]. [cit. 2018-07-11]. Dostupný z: <http://www.acr.army.cz/struktura/generalni-stab/velitelstvi-vzdusnych-sil-86864/>

ARMY.CZ, Armáda České republiky. *41. mechanizovaný prapor, historie a současnost* [online]. [cit. 2018-07-14]. Dostupný z: <http://www.41mpr.army.cz/historie-soucasnost>

ARMY.CZ, Armáda České republiky. *41. mechanizovaný prapor, struktura* [online]. [cit. 2018-07-14]. Dostupný z: <http://www.41mpr.army.cz/struktura>

ARMY.CZ, Armáda České republiky. *Výstroj* [online]. [cit. 2018-07-14]. Dostupný z: <http://www.acr.army.cz/vystroj/rukavove-znaky-vojaku-pozemnich-sil-acr-100034/>

ARMY.CZ, Armáda České republiky. *Výstroj* [online]. [cit. 2018-07-14]. Dostupný z: <http://www.acr.army.cz/vystroj/rukavove-znaky-vojaku-vzdusnych-sil-acr-100033/>

ARMY.CZ, Ministerstvo obrany ČR. *Ochrana osobních údajů v rezortu Ministerstva obrany* [online]. [cit. 2018-09-29]. Dostupný z: <http://www.mocr.army.cz/informacni-servis/povinne-informace/1-uredni-deska/ochrana-osobnich-udaju-v-resortu-ministerstva-obrany-45575/>

Clever and smart. *Analýza rizik: jemný úvod do analýzy rizik* [online]. [cit. 2018-09-05]. Dostupný z: <https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>

CNEWS.CZ, Zprávy. *Facebook má 2,1 miliardy uživatelů. Z každého má korunu denně* [online]. [cit. 2018-09-29]. Dostupný z <https://www.cnews.cz/facebook-vysledky-q4-2017>

EPRAVO.CZ – Váš průvodce právem. *Další nařízení a směrnice z dílny Bruselu – tentokrát o ochraně osobních údajů* [online]. [cit. 2018-02-21]. Dostupný z: <https://www.epravo.cz/top/clanky/dalsi-narizeni-a-smernice-z-dilny-bruselu-tentokrate-o-ochrane-osobnich-udaju-101840.html>

EPRAVO.CZ – Váš průvodce právem. *Nový návrh zákona o zpracování osobních údajů: česká adaptace GDPR a dvojitá metr při ukládání pokut?* [online]. [cit. 2018-02-22]. Dostupný z: <https://www.epravo.cz/top/clanky/novy-navrh-zakona-o-zpracovani-osobnich-udaju-ceska-adaptace-gdpr-a-dvoji-metr-pri-ukladani-pokut-106385.html>

GDPR, Obecné nařízení o ochraně osobních údajů prakticky. *Návrh nového zákona o ochraně osobních údajů je na světě* [online]. [cit. 2018-02-21]. Dostupný z: <https://www.gdpr.cz/blog/navrh-novely-zakona-c-1012000-sb-je-na-svete/>

InCOMPLIANCE v souladu s právem, Ochrana osobních údajů (GDPR). *Zabezpečení, transparentnost a minimalistické zpracování* [online]. [cit. 2018-10-11]. Dostupný z: <https://www.incompliance.cz/cz/blog/zabezpeceni-transparentnost-a-minimalisticke-zpracovani>

JEČAS.CZ. *Jaká hesla často používají čeští uživatelé* [online]. [cit. 2019-06-16]. Dostupný z <https://jecas.cz/nejcastejsi-hesla>

OSD, Odbor státního dozoru sekce dozoru a kontroly Ministerstva obrany – úřední deska. *Prohlášení GDPR* [online]. [cit. 2018-10-5]. Dostupný z: <http://www.osd.army.cz/prohlaseni-gdpr>

Novinky GDPR.cz. *Zákon o ochraně osobních údajů* [online]. [cit. 2018-02-21]. Dostupný z: <https://www.novinkygdpr.cz/ZAKON-O-OCHRANE-OSOBNICH-UDAJU/>

Vlastní cesta.cz – poradenský portál. *Metody* [online]. [cit. 2018-09-05]. Dostupný z: <https://www.vlastnicesta.cz/metody/analyza-rizik-risk/>

8 Přílohy

8.1 Příloha A Posouzení vlivu na ochranu osobních údajů

Posouzení vlivu na ochranu osobních údajů je v oblasti zpracování osobních údajů novinkou, neboť Směrnice 95/46/ES tuto problematiku doposud nezohledňovala (blíže v kapitole 4.2.1.3). Přesto, že vybraný vojenský útvar zpracovává pouze běžné, nerizikové zpracování osobních údajů, na základě čehož je od posouzení vlivu na ochranu osobních údajů zproštěn²¹⁵, z důvodu ucelenosti problematiky zpracování osobních údajů se tato příloha bude výše uvedené činnosti věnovat.

Jak uvádí čl. 35 odst. 1 Obecného nařízení 2016/679, představuje-li zpracování osobních údajů vysoké riziko pro práva a svobody fyzických osob²¹⁶, je správce či zpracovatel povinen provést posouzení vlivu na ochranu osobních údajů. Pro potřeby AČR z výše uvedeného tedy vyplývá, že v případě pravděpodobnosti vysokých rizik mezi povinnosti dílčího správce patří následující činnosti:

- 1) ujasnění účelu zpracování osobních údajů;
- 2) ujasnění právního základu pro jejich zpracování;
- 3) ujasnění rozsahu zpracovávaných osobních údajů;²¹⁷
- 4) posouzení rizik hrozících subjektu údajů z procesu zpracování osobních údajů;
- 5) stanovení předběžných organizačních a technických opatření sloužících k eliminaci možných rizik;
- 6) zpracování Zprávy o posouzení vlivu na ochranu osobních údajů;
- 7) nastavení standardů ochrany osobních údajů v dílčí evidenci;
- 8) vytvoření Záznamů o činnostech zpracování osobních údajů pro dílčí evidenci;
- 9) zaslání kopií Záznamů o činnostech státnímu tajemníkovi v MO.

²¹⁵ Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení. Viz čl. 35 odst. 1 Obecného nařízení 2016/679.

²¹⁶ Viz Článek 35 odst. 1 Obecného nařízení 2016/679 - Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

²¹⁷ Minimálně podle jejich kategorií a kategorií subjektů údajů či možné předávání jiným správcům nebo zpracovatelům.

Vyplyne-li z posouzení vlivu na ochranu osobních údajů, že by dané zpracování mělo za následek vysoké riziko v případě, že by nebyly přijaty opatření ke zmírnění tohoto rizika, stává se navazující povinností správce předchozí konzultace s dozorovým orgánem.²¹⁸ Při konzultaci s dozorovým úřadem správce dokládá účel a způsob zamýšleného zpracování, ve vhodných případech rozdělení odpovědnosti správce, společných správců a zpracovatelů zapojených do zpracování či opatření a záruky poskytnuté za účelem ochrany práv a svobod subjektů údajů. Mezi další požadované informace patří kontaktní údaje na pověřence pro ochranu osobních údajů, zpracované posouzení vlivu správcem a veškeré další informace, o které dozorový úřad požádá.²¹⁹

8.1.1 Účel zpracování osobních údajů

Základem zpracování osobních údajů a souvisejících povinností pro správce je účel zpracování. Správné posouzení účelu zpracování výrazně ulehčí, v případě špatného posouzení zkomplikuje, všechny následující kroky. Na účel zpracování jsou vázány zásady zpracování a povinnosti plynoucí z ustanovení Obecného nařízení 2016/679 (blíže v kapitole 4.2.1.2).

Správce může účel zpracování osobních údajů stanovit přímo nebo může účel představovat soubor jeho činností, pro něž potřebuje zpracovávat osobní údaje. U zaměstnanců rezortu MO dochází ke zpracování osobních údajů prostřednictvím správce či zpracovatele v rozsahu a pro účel vyplývající z obecně závazných právních předpisů, viz tabulka 16.

Účelem lze chápat povinnost například při ochraně majetku státu, zabezpečení ochrany utajovaných informací, vedení účetní evidence či vynakládání finančních prostředků k naplnění povinnosti dle smluvního vztahu (vojákoví z povolání, zaměstnanci nebo smluvnímu partnerovi).

²¹⁸ Článek 36 odst. 1 Obecného nařízení 2016/679.

²¹⁹ Článek 36 odst. 3 písm. f) Obecného nařízení 2016/679.

Tabulka 16 Rozsah a účel zpracování osobních údajů v rezortu MO

Právní předpisy ve znění pozdějších předpisů:	
zák. č. 451/1991 Sb.	kterým se stanoví některé další předpoklady pro výkon některých funkcí ve státních orgánech a organizacích
zák. č. 582/1991 Sb.	o organizaci a provádění sociálního zabezpečení
zák. č. 586/1992 Sb.	o daních z příjmu
zák. č. 48/1997 Sb.	o veřejném zdravotním pojištění
zák. č. 221/1999 Sb.	o vojácích z povolání
zák. č. 133/2000 Sb.	o evidenci obyvatel
zák. č. 187/2006 Sb.	o nemocenském pojištění
Prováděcí právní předpisy ve znění pozdějších předpisů:	
NV č. 590/2006 Sb.	kterým se stanoví okruh a rozsah jiných důležitých osobních překážek v práci
NV č. 332/2014 Sb.	kterým se mění zákon č. 221/1999 Sb., o vojácích z povolání ve znění pozdějších předpisů, a další související zákony
NV č. 341/2017 Sb.	o platových poměrech zaměstnanců ve veřejných službách a správě
Vyhlášky:	
Vyhl. č. 263/1999 Sb.	kterou se stanoví důvody pro poskytování služebního volna VzP pro překážky ve službě a rozsah služebního volna
Vyhl. č. 264/1999 Sb.	o poskytování studijního volna VzP
Vyhl. č. 265/1999 Sb.	kterou se stanoví doba setrvání ve služebním poměru VzP, kteří se připravují k výkonu služby studiem, a výše úhrady, kterou lze na VzP požadovat, pokud nesplní dohodu
Vyhl. č. 454/2002 Sb.	kterou se stanoví doklady pro výběr, postup při výběru a vzor osobního dotazníku uchazeče o povolání do služebního poměru VzP
Vyhl. č. 114/2002 Sb.	o fondu kulturních a sociálních potřeb

Zdroj: zpracováno dle ARMY.CZ, Ministerstvo obrany ČR. *Ochrana osobních údajů v rezortu Ministerstva obrany* [online]. [cit. 2018-09-29]. Dostupný z: <http://www.mocr.army.cz/informacni-servis/povinne-informace/1-uredni-deska/ochrana-osobnich-udaju-v-resortu-ministerstva-obrany-45575/>

V praxi se lze setkat se situací, kdy pro jednu množinu osobních údajů může existovat více účelů zpracování. Pozbytí možnosti jednoho účelu zpracování nemusí znamenat nutnou likvidaci dat, protože dané údaje mohou být zpracovány pro další účely. Na základě výše uvedeného poté dochází k případům, že jsou osobní údaje subjektu údajů zpracovány v rozdílné míře pro různé účely, tzn. každý účel v jiném rozsahu.²²⁰

²²⁰ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 56.

8.1.2 Právní základ zpracování osobních údajů

Právní důvod znamená právním řádem předpokládané oprávnění ke zpracování osobních údajů ze strany správce za legitimním účelem. Jak již uvádí kapitola 4.2.1.2 (Dodržování zásad zpracování osobních údajů), zpracování je zákonné pouze v případě, je-li splněna nejméně jedna z podmínek uvedených v čl. 6 odst. 1 Obecného nařízení 2016/679 a pouze v odpovídajícím rozsahu.

V rezortu MO dochází nejčastěji ke zpracování osobních údajů na základě splnění podmínky nezbytnosti zpracování pro splnění právní povinnosti, která se na správce vztahuje²²¹. V tomto případě je nutností přesná identifikace ustanovení právního předpisu, ze kterého povinnost zpracovávat osobní údaje plyne.²²²

Další uplatňovanou podmínkou je nezbytnost zpracování osobních údajů pro splnění úkolu prováděného ve veřejném zájmu či při výkonu veřejné moci, kterým je pověřen správce.²²³ Jedná se o případy výkonu svěřené veřejnoprávní působnosti jednotlivým útvarům rezortu MO, a to například zpracování v souvislosti s kázeňskou a kárnou pravomocí.

V neposlední řadě nelze opomenout zpracování osobních údajů v souvislosti s ochranou životně důležitých zájmů subjektů údajů nebo jiných fyzických osob.²²⁴ V armádě ČR lze tuto podmínku uplatnit v případech souvisejících s nasazením vojáků v krizových oblastech nebo v případě přímého ohrožení života či zdraví osob.

S podklady pro zpracování osobních údajů dále úzce souvisí i čl. 13 Obecného nařízení 2016/679, který obsahuje výčet informací, které musí správce poskytnout subjektu údajů v okamžiku, kdy od něj získává osobní údaje. Výčet zahrnuje následující informace:

- a) totožnost a kontaktní údaje správce a jeho případného zástupce;*
- b) kontaktní údaje na pověřence pro ochranu osobních údajů;*
- c) účel zpracování, pro který jsou osobní údaje určeny, a právní základ pro zpracování;*

²²¹ Článek 6 odst. 1 písm. c) Obecného nařízení 2016/679.

²²² Podle toho ustanovení není možné postupovat v případě, má-li zpracování osobních údajů oporu pouze ve vnitřním předpise.

²²³ Článek 6 odst. 1 písm. e) Obecného nařízení 2016/679.

²²⁴ Článek 6 odst. 1 písm. d) Obecného nařízení 2016/679.

- d) oprávněné zájmy správce nebo třetí strany v případě, jedná-li se o zpracování dle čl. 6 odst. 1 písm. f) Obecného nařízení 2016/679;²²⁵*
- e) případné příjemce nebo kategorie příjemců osobních údajů;*
- f) případný úmysl správce předat osobní údaje do třetí země nebo mezinárodní organizaci.²²⁶*

Vedle výše uvedených informací je dle čl. 13 odst. 2 Obecného nařízení 2016/679 správce povinen subjektu údajů poskytnout ještě další informace, jsou-li nezbytné k zajištění spravedlivého a transparentního zpracování.²²⁷

V případě, že je právním podkladem zpracování výkon veřejné moci, plnění úkolů ve veřejném zájmu nebo je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, má subjekt údajů možnost vznést dle čl. 21 Obecného nařízení 2016/679²²⁸ námitku proti zpracování. Správce je poté oprávněn pokračovat ve zpracování pouze za předpokladu, že prokáže závažné oprávněné důvody, které převažují nad zájmy nebo právy a svobodami subjektu údajů.

Povinností dílčího správce po celou dobu zpracování osobních údajů je tedy zachování proporcionality mezi veřejným zájmem a zachováním základních práv a svobod subjektu údajů.

²²⁵ Zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.

²²⁶ Článek 13 odst. 1 Obecného nařízení 2016/679.

²²⁷ a) *doba, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá pro stanovení této doby;*

b) *existence práva požadovat od správce postup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vnést námitku proti zpracování, jakož i práva na přenositelnost údajů;*

c) *pokud je zpracování založeno na udělení souhlasu subjektem údajů, existence práva odvolat kdykoliv souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním;*

d) *existence práva podat stížnost u dozorového úřadu;*

e) *skutečnost, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů;*

f) *skutečnost, že dochází k automatizovanému rozhodování, včetně profilování a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů. Viz čl. 13, odst. 2 Obecného nařízení 2016/679.*

²²⁸ Článek 21 Obecného nařízení 2016/679 - Právo vznést námitku.

8.1.3 Rozsah zpracovaných osobních údajů

Rozsah zpracovaných osobních údajů souvisí s další zásadou Obecného nařízení 2016/679, a to s minimalizací údajů (blíže v kapitole 4.2.1.2 Dodržování zásad zpracování osobních údajů). Jedná se o ochranu bránící správci, aby v souvislosti s legitimním účelem poptával po subjektu údajů více informací, než je nezbytné.

Dílčí správce v AČR je tedy povinen u každého údaje posoudit, zda jeho zpracování opravdu potřebuje, a toto své rozhodnutí musí být schopen obhájit. Obhajoba bude podložena konkrétní právní nebo smluvní povinností, popř. věcnou potřebou k naplnění této povinnosti. Osobní údaje musí být rozděleny dle kategorií subjektů údajů (např. voják z povolání, voják v aktivní záloze, občanský zaměstnanec, zaměstnanec smluvního partnera, žadatel apod.) a dále podle kategorií jednotlivých údajů (např. identifikační, průběh služby, zabezpečení nakládání s majetkem, zabezpečení provozu vojenských vozidel, plnění smluvních povinností apod.).

Zásadní je také ujasnění, zda při zpracování osobních údajů nebude docházet k jejich předání mimo rezort MO, zda se na jejich zpracování nebudou podílet i jiné subjekty nebo zda osobní údaje nebudou v nějaké podobě předávány systematicky jinému správci.

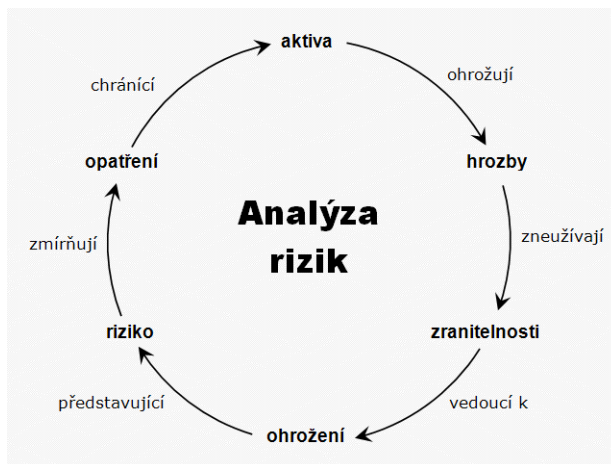
Přestože je zásada minimalizace údajů univerzální, mohou ji některé zvláštní právní předpisy zdůrazňovat, jako např. zákon č. 262/2006 Sb., zákoník práce ve znění pozdějších předpisů, který v § 30 odst. 2 stanovuje, že v souvislosti s jednáním před vznikem pracovního poměru smí zaměstnavatel vyžadovat od uchazečů pouze ty údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy.²²⁹

8.1.4 Posouzení rizik hrozících subjektu údajů z procesu zpracování osobních údajů

V případě, hrozí-li při zpracování osobních údajů vysoké riziko, je správce MO povinen přijmout taková opatření, která umožní rizika zvládat, snížit či zcela eliminovat. Jak stanovuje RMO č. 22/2018, jedním z úkonů, které musí dílčí správce zabezpečující plnění povinností ministerstva v dílčí evidenci provést, je analýza rizik a jejich hodnocení. Ilustrační schéma možné analýzy zobrazuje následující obrázek.

²²⁹ ŽŮREK, J. *Praktický průvodce GDPR*. 2017, s. 61.

Obrázek 10 Schéma analýzy rizik²³⁰



Zdroj: <https://www.cleverandsmart.cz/analýza-rizik-jemny-uvod-do-analýzy-rizik/>

Prvním úkolem dílčího správce je tedy identifikace rizik, jejich posouzení a předběžné rozhodnutí o jejich řízení, což zahrnuje přijetí opatření ke snížení, odstranění, převedení či přijmutí rizika. Riziko definují dva komponenty, a to hrozba (která působí) a zranitelnost (kterou hrozba využije). V oblasti zpracování osobních údajů se může jednat o náhodné zničení, neoprávněné zpřístupnění, pozměňování či například ztrátu. Při prvotním posouzení je třeba kromě hrozby a zranitelnosti dále zohlednit možný dopad, který tato hrozba způsobí, a pravděpodobnost výskytu hrozby.

Jak již bylo zmíněno, dílčí správce je osobou odpovědnou za hodnocení rizik z toho důvodu, že je s osobními údaji nejlépe obeznámen a je schopen stanovení jednotlivých atributů a objektivního hodnocení. Pravděpodobnost a závažnost rizika je povinen posoudit na základě rozsahu, kontextu, účelu zpracování a v neposlední řadě na způsobu

²³⁰ Vysvětlení pojmů užitých v obrázku 10:

Aktivum – vše co má pro společnost nějakou hodnotu a mělo by být odpovídajícím způsobem chráněno (v našem případě osobní údaje).

Hrozba – jakákoliv událost, která může způsobit narušení důvěrnosti, integrity a dostupnosti aktiva.

Zranitelnost – vlastnost aktiva nebo slabina na úrovni fyzické, logické nebo administrativní bezpečnosti, která může být zneužita hrozbou.

Riziko – pravděpodobnost, že hrozba zneužije zranitelnost a způsobí narušení důvěrnosti, integrity nebo dostupnosti.

Opatření – opatření na úrovni fyzické logické nebo administrativní bezpečnosti, které snižuje zranitelnost a chrání aktivum před danou hrozbou

shromažďování osobních údajů. Výsledkem posouzení by měla být identifikace zranitelnosti osobních údajů, identifikace hrozby a určení dopadu.²³¹

Po zpracování analýzy rizik je dílčí správce povinen navrhnout taková organizační a technická opatření, aby zjištěná rizika minimalizoval. Dle hierarchie rezortu MO poté dochází k převzetí hodnocení rizik a přijatých opatření vedoucím organizačního celku spadajícím do působnosti dílčího správce a jejich aplikace do praxe. Rozhodne-li vedoucí organizačního celku o vedení vlastní agendy obsahující osobní údaje, je povinen provést stejné úkony, které jsou výše uvedeny pro dílčího správce.

Přijmutí organizačních a technických opatření vede buď ke snížení pravděpodobnosti aktivace rizika, nebo ke snížení negativních dopadů souvisejících s aktivací. Aplikaci organizačních a technických opatření je nutné zaznamenat do vytvořené analýzy a hodnocení rizik a zjistit dopady na jednotlivá uvedená rizika. Výsledkem bude zápis nových hodnot pravděpodobnosti výskytu rizika a míry dopadu, čímž dojde ke změně klasifikace úrovně. Výsledky analýzy se stanou součástí Zprávy o posouzení vlivu zpracování osobních údajů a ta bude dle čl. 6 odst. 1 RMO č. 22/2018 směřována ke stanovisku pověřenci pro ochranu osobních údajů a pro informaci státnímu tajemníkovi v MO.

8.1.5 Stanovení předběžných organizačních a technických opatření

Jak již bylo zmíněno v předchozí kapitole, organizační a technická opatření slouží k eliminaci rizik při zpracování osobních údajů. Pro potřeby rezortu článek 8 odst. 3 RMO č. 22/2018 definuje následující výčet opatření:

- a) *bezpečnostní politika činností zpracování osobních údajů;*
- b) *organizační požadavky na činnosti zpracování;*
- c) *požadavky na zaměstnance vykonávající činnosti zpracování;*
- d) *řízení přístupu osob ke zpracovaným osobním údajům a jejich rozsahu;*
- e) *fyzické zabezpečení osobních údajů;*
- f) *požadavky na nástroje elektronické podpory činnosti zpracování;*
- g) *využití nástrojů pro ověřování identity uživatelů a řízení jejich přístupu k nástrojům elektronické podpory činností zpracování.*²³²

²³¹ Při hodnocení možného dopadu se přihlíží k nejkritičtějším možným scénářům s maximálními dopady. Především je nutné zohlednit vliv na dostupnost, důvěrnost či integritu osobních údajů

Rozhodnutí ohledně vhodných organizačních a technických opatření je v režii dílčího správce, který musí vycházet z konkrétních rizik a podmínek zpracování. Dle svého subjektivního rozhodnutí může za opatření dále považovat:

- pseudonymizaci či anonymizaci osobních údajů;
- vhodné nastavení procesů ve věcné agendě;²³³
- proškolení zaměstnanců vzhledem k povinnosti mlčenlivosti, požadované tvorby hesel;
- nastavení procesů při změně zařazení zaměstnanců či při ukončení služebního poměru;
- zabezpečení uložených dat proti zničení.

Současný stav nařízených opatření k ochraně osobních údajů²³⁴ bude dílčímu správci nápomocen při přechodu na plnění povinností plynoucích z Obecného nařízení 2016/679. Dílčí správce se sice nevyhne přezkoumání původně platných opatření v porovnání s novými zásadami plynoucími z nařízení, ale celý postup bude mít výrazně jednodušší.

8.1.6 Zpráva o posouzení vlivu na ochranu osobních údajů

Zpráva o posouzení vlivu na ochranu osobních údajů je souhrnem všech předchozích kroků. Vhodné je, aby dále obsahovala co nejvíce informací potřebných pro zpracování následujícího dokumentu, a to Záznamu o činnostech zpracování, který vyžaduje Obecné nařízení 2016/679.²³⁵

Pro potřeby sjednocení postupů v oblasti zpracování osobních údajů v rezortu MO je úkolem pověřence pro ochranu osobních údajů a státního tajemníka provést posouzení vytvořených zpráv. Jejich úkolem je kromě metodické pomoci také zabezpečení shody mezi činnostmi v rámci rezortu, ÚOOÚ a s praxí mimo rezort. Výsledkem provedení výše uvedených úkonů je shoda v obsahu Zprávy o posouzení vlivu osobních údajů, v opačném případě je povinností pověřence předložit rozpor k řešení přímo ministrovi obrany.

Jak již bylo zmíněno výše, dalším potřebným dokumentem je Záznam o činnostech zpracování, který do jisté míry představuje náhradu za původní oznamovací povinnost

²³² Článek 8 odst. 3 RMO č. 22/2018 – Nastavení standardů ochrany osobních údajů v dílčích evidencích.

²³³ Snížení počtu zaměstnanců zapojených do zpracování osobních údajů na nezbytně nutné množství.

²³⁴ Dle zákona č. 101/2000 Sb. a RMO č. 16/2013.

²³⁵ Dle čl. 30 Obecného nařízení 2016/679 – Záznamy o činnostech zpracování.

a umožňuje správci prokázat soulad zpracování osobních údajů s Obecným nařízením 2016/679.²³⁶ Záznamy o činnostech zpracování musí dle evropského nařízení obsahovat:

- 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;*
- f) *je-li to možné, plánované lhůty pro výmaz jednotlivých kategorií údajů;*
- g) *je-li to možné, obecný popis technických a organizačních bezpečnostních opatření.*²³⁷

Kromě výše uvedených náležitostí je v RMO č. 22/2018 výčet dále rozšířen o:

- a) *popis způsobu shromažďování jednotlivých kategorií osobních údajů;*
- b) *popis způsobu poučení subjektu osobních údajů o zpracování jeho údajů ve smyslu čl. 13 Obecného nařízení 2016/679;*²³⁸
- c) *popis způsobu uchování dokladů o právním důvodu zpracování osobních údajů;*
- d) *popis organizačních a technických opatření k ochraně osobních údajů;*
- e) *pravidla pro periodické hodnocení jejich nezbytnosti a efektivnosti.*²³⁹

Prioritou zpracovaných Záznamů o činnostech zpracování je nařízení vhodných organizačních a technických opatření k ochraně osobních údajů. Závěrečnou povinností pro dílčího správce je odeslání zpracovaných Záznamů o činnostech zpracování státnímu tajemníkovi v MO.

²³⁶ NEZMAR, L. *GDPR: Praktický průvodce implementací*. 2017, s. 31.

²³⁷ Článek 30 odst. 1 Obecného nařízení 2016/679.

²³⁸ Článek 13 Obecného nařízení 2016/679 - Informace poskytované v případě, že osobní údaje jsou získány od subjektu údajů.

²³⁹ Článek 8 odst. 2 RMO č. 22/2018.

8.2 Příloha B Jmenovitá evidence

Tabulka 17 Členění jmenovité evidence

Osobní doklady	
Osobní spis	slouží k provádění personální práce s fyzickými osobami a k zakládání veškeré pers. dokumentace zpracované v průběhu služebního poměru
Pomocný osobní spis	představuje souhrn údajů o průběhu činné služby. Slouží k vedení centrální personální evidence a jako podklad pro vedení evidence za stavu ohrožení státu nebo válečného stavu
Výkaz dob pro zabezpečení peněžitými dávkami a pro důchodové pojištění	slouží k přesnému vykazování dob vojenské služby pro účely výluhových náležitostí a důchodového pojištění
Identifikační doklady	
Vojenský průkaz	vojákům se vydává k prokazování jejich příslušnosti k ozbrojeným silám ČR
Osobní známka	určena k identifikaci fyzických osob ve stavu ohrožení státu, za válečného stavu nebo při vyslání ke službě v zahraničí
Personální dokumentace	
Rozhodnutí služebního orgánu	právní dokument, kterým příslušný služební orgán uskutečňuje některá personální opatření
Personální rozkaz	právní dokument, kterým služební orgán uskutečňuje personální opatření ve věcech služebního poměru
Výnos služebního orgánu ve věcech personálních	vydává služební orgán k zabezpečení úkolů personální evidence
Podnět k personálnímu opatření	služební orgán jím navrhuje provedení personálního opatření s fyzickými osobami
Oznámení osobní změny	osoby oznamují změny v osobních údajích za sebe a osoby blízké
Osobní dotazník a životopis	slouží k získání základních osobních údajů a poznatků o fyzické osobě a jeho blízkých osobách
Potvrzení o délce výkonu vojenské činné služby	služební orgán v něm při zániku služebního poměru potvrzuje délku výkonu vojenské činné služby a další údaje stanovené zákonem
Určovací lístek	slouží jako doklad při přeložení, odvelení a při zániku služebního poměru vojáka
Záznam o pohovoru	obsah a výsledek pohovoru osoby se služebním orgánem
Dohoda o zvýšení nebo rozšíření vzdělání	v rámci studia, vzdělávání, školení nebo jiné formy přípravy k dosažení vyššího stupně vzdělání
Služební hodnocení	periodicky zpracováváný dokument
Písemné hodnocení při zániku služebního poměru	nezbytný dokument při ukončení služebního poměru
Oznámení o obdržení Osvědčení fyzické osoby vydávané NBÚ ²⁴⁰	ve smyslu § 11 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti ve znění zákona č. 255/2011 Sb.
Popis pracovní činnosti zaměstnance	seznámení osob se všemi podstatnými činnostmi a úkoly vztahujícími se k jeho služebnímu zařazení
Záznam o pořízení kopie (opisu, výpisu)	včetně uvedení za jaké části osobního dokladu byla kopie pořízena, pro jaký účel, kdo pořízení povolil a převzal

²⁴⁰ NBÚ – Národní bezpečnostní úřad.

Evidenční pomůcky	
Abecední kniha	obsahuje přehledové listy o osobách v podřízenosti v abecedním pořadí, se základními služebními a osobními údaji a záznamy o pohybu osobních údajů
Deník personálních opatření	slouží k evidenci vydávaných rozhodnutí, personálních rozkazů a výnosů ve věcech personálních příslušného služebního orgánu
Kniha přijatých personálních opatření	slouží k evidenci rozhodnutí, personálních rozkazů a výnosů ve věcech personálních od nadřízených služebních orgánů
Kartotéka vojáků vyřazených z evidence	vedena z pomocných osobních spisů
Kartotéční lístek studujícího vojenské školy	určen k sestavení abecední kartotéky, která dává přehled o všech studujících, kteří ve škole sudovali a studují
Kniha systemizovaných míst	dává přehled o systemizovaných místech v celé podřízenosti daného stupně a jejich obsazenosti
Inventární kniha osobních čísel	dává přehled o vydaných osobních číslech fyzických osob
Přehled VzP s přerušeným služebním poměrem	dává přehled o VzP, u kterých došlo k přerušení služebního poměru

Zdroj: zpracováno dle RMO 114/2014 Personální evidence vojáků z povolání občanských zaměstnanců a zaměstnanců ve správních úřadech

8.3 Příloha C Prohlášení MO o zpracování osobních údajů²⁴¹

Prohlášení o zpracování osobních údajů dle nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a poučení subjektů údajů (dále jen „GDPR“).

I. Správce osobních údajů - správcem osobních údajů pro oblast dozoru a kontroly v rezortu Ministerstva obrany je Ing. Antonín Rada, náměstek pro řízení sekce dozoru a kontroly MO, Tychonova 1, 160 00 Praha

Pověřenec pro ochranu osobních údajů:

- Mgr. Lucie Kazdová, tel. 973 229 328, e-mail: kazdoval@army.cz
- Mgr. Ing. Andrea Ligačová, MBA, tel. 973 229 324, e-mail: ligacovaa@army.cz

II. Zdroje osobních údajů

- přímo od subjektů údajů;
- veřejně přístupné rejstříky, seznamy a evidence (např. katastr nemovitostí, obchodní rejstřík, živnostenský rejstřík apod.).

III. Kategorie osobních údajů, které jsou předmětem zpracování

- adresní a identifikační údaje sloužící k jednoznačné a nezaměnitelné identifikaci subjektu údajů (např. jméno, příjmení, titul, hodnost, příp. rodné číslo, datum narození, adresa trvalého pobytu, IČ, DIČ) a údaje umožňující kontakt se subjektem údajů (kontaktní údaje – např. kontaktní adresa, číslo telefonu, číslo faxu, emailová adresa a jiné obdobné informace);
- údaje poskytnuté nad rámec příslušných zákonů zpracovávané v rámci uděleného souhlasu ze strany subjektu údajů.

IV. Rozsah a účel zpracování osobních údajů

Správce zpracovává osobní údaje subjektů v souladu s obecně závaznými právními předpisy zejména s „GDPR“.

Zpracování osobních údajů je nezbytné pro splnění úkonů prováděných ve veřejném zájmu nebo při výkonu veřejné moci, kterou je pověřen správce.

Osobní údaje jsou určeny k identifikaci subjektů údajů v rozsahu, v jakém je příslušný subjekt údajů správcem poskytl a jak jsou stanoveny příslušnými právními předpisy.

Jedná se zejména o tyto právní předpisy:

- zákon č. 500/2004 Sb., správní řád;
- zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich;
- zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon);

²⁴¹ OSD, Odbor státního dozoru sekce dozoru a kontroly Ministerstva obrany – úřední deska. *Prohlášení GDPR* [online]. [cit. 2018-10-5]. Dostupný z: <http://www.osd.army.cz/prohlaseni-gdpr>

- zákon č. 406/2000 Sb., o hospodaření energií;
- zákon č. 133/1985 Sb., o požární ochraně;
- zákon č. 219/1999 Sb., o ozbrojených silách;
- zákon č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci).

V. Způsob zpracování a ochrany osobních údajů

Zpracování osobních údajů provádí správce. Zpracování je prováděno na jednotlivých pracovištích pověřenými nebo určenými zaměstnanci správce. Ke zpracování dochází prostřednictvím výpočetní techniky, popř. i manuálním způsobem u osobních údajů v listinné podobě při dodržení všech bezpečnostních zásad pro správu a zpracování osobních údajů. Za tímto účelem přijal správce organizační opatření k zajištění ochrany osobních údajů, zejména opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Zpracovatelé osobních údajů, kterým mohou být a jsou osobní údaje zpřístupněny, respektují právo subjektů údajů na ochranu soukromí a jsou povinni postupovat dle platných právních předpisů týkajících se ochrany osobních údajů.

VI. Doba zpracování a uložení osobních údajů

V souladu se spisovým a skartačním řádem správce a příslušnými právními předpisy. Osobní údaje jsou ukládány dlouhodobě pro potřebu doložení informací podle výše uvedených právních předpisů. V případě osobních údajů použitých při výkonu činností podle stavebního zákona po celou dobu existence stavby.

VII. Práva subjektů údajů

a) V souladu se zpracováním osobních údajů má subjekt údajů níže uvedená práva. Na výkon těchto práv se vztahují výjimky, proto není možné je uplatnit ve všech situacích. V případě, že subjekt údajů uplatní svá práva a jeho žádost bude shledána oprávněnou, správce přijme požadovaná opatření bez zbytečného odkladu. Práva subjektu údajů:

- právo na přístup k osobním údajům;
- právo na opravu;
- právo odvolat souhlas;
- právo vznést námitku;
- právo na omezené zpracování;
- právo na přenositelnost údajů.

b) V souladu se čl. 12 GDPR informuje správce subjekt údajů na základě jeho žádosti o právu na přístup k osobním údajům a k následujícím informacím:

- účelu zpracování;
- kategorii dotčených osobních údajů;

- příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny;
- plánované době, po kterou budou osobní údaje uloženy;
- veškeré dostupné informace o zdroji osobních údajů;

c) Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může:

- požádat správce o vysvětlení
- požadovat, aby správce odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo vymazání osobních údajů.

V případě, že se subjekt údajů domnívá, že jsou jeho osobní údaje zpracovávány v rozporu s právními předpisy, má právo obrátit se na správce s žádostí o sjednání nápravy. Tento postup nevylučuje, aby se subjekt údajů přímo obrátil se svým podnětem nebo stížností na dozorový úřad – Úřad pro ochranu osobních údajů.

Správce má právo za poskytnutí informace požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace.

8.4 Příloha D Upřesnění práce s osobními údaji v účetních evidencích FIS²⁴²

Při evidenci dokumentů v účetních modulech FIS (POZ, POK, POU, PRE, KDF, KOF, UCT, FUC a MUD)²⁴³ je pro splnění požadavků Nařízení Evropského parlamentu a rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (tzv. GDPR) nutné upravit pravidla pro nakládání s osobními údaji. V tomto smyslu je v každém konkrétním případě žádoucí ujasnit si, zda je použití osobního údaje nezbytné pro další zpracování účetního případu a v jakém rozsahu.

Základní pravidlo zní:

NEPOUŽÍVAT OSOBNÍ ÚDAJE NEUVEDENÉ V EXTERNÍM SUBJEKTU DANÉHO PŘÍPADU (až na níže uvedené výjimky).

Poznámka: Pokud je v poli Externí subjekt (ESU) uvedena fyzická osoba a její osobní údaje se vyskytují i v jiných částech stejného dokladu (v popisu, v poznámce, na přílohách), není nutné znovu uvádět tuto osobu do Dotčených subjektů. Zároveň není nutné její osobní údaje z evidencí odstraňovat.

Pokud je z legislativních důvodů nezbytné uvádět do účetní evidence (popis, poznámka, přílohy) osobní údaje osoby, která není uvedena na stejném dokladu v ESU, je nutné tuto osobu uvést do Dotčených subjektů daného dokladu (na dokladu v horní liště tlačítko „Vazby“ – „Dotčené subjekty“).

Osobní údaje identifikující zpracovatele, vlastníky dokladů nebo schvalující funkcionáře uváděné na dokladech nebo v přílohách není nutné odstraňovat ani evidovat v dotčených subjektech.

Ve všech ostatních případech je zakázáno uvádět:

- v popisech a poznámkách dokladů jména a další osobní údaje,
- v přílohách jmenné seznamy osob (slouží pro potřebu daných nákladových středisek. Pokud je seznam přílohou faktury, nákladové středisko seznam oddělí a do účetnictví nepředkládá),
- v přílohách kopie emailových nebo jiných komunikací,
- v přílohách kopie smluv (tyto jsou uvedeny v modulu SML).

Pokud budou tyto údaje při evidenci dokumentů z úrovně nákladového střediska zadány, musí být před zaúčtováním dokladu z úrovně účetní Agentury finanční odstraněny.

²⁴² Finanční informační systém

²⁴³ POZ - Pokladna zálohová, POK – Pokladna, POU – Kniha poukazů, PRE – Kniha převodných poukazů, KDF – Kniha došlých faktur), KOF – Kniha odeslaných faktur, UCT – Pořizovač účetních dokladů, FUC – Finanční účtárna, MUD – Pořizovač materiálních účetních dokladů

Z tohoto důvodu je nutné pracovat správně s elektronickými přílohami. Nejdůležitější podkladový účetní záznam je zobrazen jako „Elektronický obraz“ (např. samotná faktura), ostatní podkladové účetní záznamy jsou uvedeny jako „Přílohy“, kterých může být více.

Konkrétní příklady osobních údajů, které byly v rámci analýzy osobních údajů v jednotlivých modulech zjištěny a které není možné dále v rámci účetní evidence dokladů v modulech FIS uvádět:

Modul KDF (Kniha došlých faktur), KOF (Kniha odeslaných faktur)

- osobní údaje v popisech faktur (případně uvádět v dotčených subjektech),
- v rámci příloh jmenné seznamy strážníků, účastníků pohoštění, ubytovaných osob apod. (v případě úhrady stravy, bude uvedena pouze soupiska z modulu PDM),
- v případě faktur na čerpání z FKSP, na kterých jsou spolu se zaměstnancem uvedeny i další oprávněné osoby většinou pouze ve tvaru „jméno a příjmení“, bude v dotčených subjektech uveden pouze daný zaměstnanec (tento případ je dále v řešení s dodavatelskou firmou).

Modul POZ (Pokladna zálohová), POK (Pokladna)

- v rámci příloh kopie smluv, kopie pokladní knihy, apod.,
- v popisu osobní údaje různých osob (případně uvádět v dotčených subjektech),
- v případě osob přebírajících hotovost na základě plné moci je nutné uvést tuto osobu do dotčených subjektů,
- v případě přikládání výplatních listin se seznamy osob, které hotovost přebírají, se tyto listiny do FIS neskenují a osoby na nich uvedené se neuvádějí do dotčených subjektů. Výplatní listina je součástí účetního dokladu pouze v listinné podobě.

Modul POU (Kniha poukazů), PRE (Kniha převodných poukazů)

- v rámci příloh jmenné seznamy strážníků apod.,
- v rámci příloh výpis registru ekonomických subjektů,
- v rámci popisu jména zaměstnanců (případně uvádět v dotčených subjektech),
- v přílohách, kde jsou např. v rámci rozsudků uvedené osoby, tyto uvést v dotčených subjektech (pokud je vůbec nutné rozsudky vkládat, dostačující by měl být např. odkaz na doklad v DDP – Daně, dávky, poplatky),
- v přílohách u transferů (rozhodnutí o poskytnutí dotace apod.) pověřené, kontaktní, odpovědné a spolupodílející se osoby na projektu (případně uvádět v dotčených subjektech).

Modul MUD (Pořizovač materiálních účetních dokladů)

- u vybraných druhů pohybů majetku je nutná věcná kontrola účetní příslušné účtárny v Informačním systému logistiky. Účetní mimo jiné prověří, zda v poznámce (v odůvodnění) nejsou uvedeny osobní údaje. V případě, že na podkladovém účetním záznamu budou osobní údaje uvedeny, dávku odmítne

- s popisem: „Vzhledem k platnosti Nařízení GDPR je zakázáno uvádět osobní údaje“. Zhotovitel podkladového účetního záznamu osobní údaje odstraní,
- ve výkazech vydaného materiálu je možné uvádět zaměstnance, který materiál přebírá.

Modul UCT (Pořizovač účetních dokladů)

- v popisu osobní údaje (případně uvádět v dotčených subjektech),
- v rámci příloh emailové komunikace.

8.5 Příloha E Poučení o zpracování osobních údajů o.z. před nabytím účinnosti Obecného nařízení 2016/679²⁴⁴

Osobní číslo zaměstnance:

.....

INFORMACE

pro pan(i)

(podle § 11 zákona č. 101/2000 Sb., o ochraně osobních údajů)

Prohlašuji, že jsem byl(a) poučena(a) o tom, že mnou povinně poskytnuté osobní údaje jsou (budou) zpracovávány služebními orgány zaměstnavatele – Ministerstva obrany ČR – nebo jinou právníckou osobou jako smluvní partnerem zaměstnavatele v rozsahu a pro účel vyplývající z obecně závazných právních předpisů, zejména:

- zákona č. 48/1997 Sb., o veřejném zdravotním pojištění (např. § 10 odst. 1, písm. a)²⁴⁵,
- zákona č. 586/1992 Sb., o daních z příjmu (např. §35ba, § 35c)²⁴⁶,
- zákona č. 133/2000 Sb., o evidenci obyvatel (např. § 13c)²⁴⁷,
- zákona č. 582/1991 Sb., o organizaci a provádění sociálního zabezpečení ve znění pozdějších předpisů (např. § 37)²⁴⁸,
- zákona č. 451/1991 Sb., tzv. lustrační zákon (§ 3),
- nařízení vlády č. 590/2006 Sb., kterým se stanoví okruh a rozsah jiných důležitých osobních překážek v práci,
- nařízení vlády č. 564/2006 Sb., o platových poměrech zaměstnanců ve veřejných službách a správě,
- vyhlášky Ministerstva financí č. 114/2002 Sb., o FKSP, aj.

Poskytnuté osobní údaje bude v souvislosti s pracovním poměrem soustřeďovat a vést personalista organizačního celku, u kterého budu (jsem) zařazen(a) a příslušný orgán finančně ekonomické služby zaměstnavatele. Osobní údaje jsou vedeny v listinné podobě na formulářích, které jsem dobrovolně vyplnil(a) v souvislosti s uzavřením pracovního poměru. Na jejich základě budou zároveň vedeny v elektronické podobě v Informačním systému o službě a personálu (dále jen „ISSP“). Moje osobní údaje mohou být

²⁴⁴ Formulář z Informačního systému o službě a personálu.

²⁴⁵ § 10 odst. 1, písm. a - Zaměstnavatel je povinen nejpozději do osmi dnů od vzniku skutečnosti, která se oznamuje, provést u příslušné zdravotní pojišťovny oznámení o: a) nástupu zaměstnance do zaměstnání a jeho ukončení; jde-li o pojištěnce podle § 2 odst. 1 písm. b), oznamuje též tuto skutečnost.

²⁴⁶ § 35ba - Slevy na dani pro poplatníky daně z příjmů fyzických osob, § 35c - Daňové zvýhodnění pro poplatníky daně z příjmů fyzických osob.

²⁴⁷ § 13c - Využívání rodných čísel.

²⁴⁸ § 37 - Vedení a předkládání záznamů.

zpřístupněny pouze vedoucím zaměstnancům, kteří mi jsou (budou) nadřizení, personálním a finančním orgánům zaměstnavatele a dalším osobám stanoveným v ustanovení § 312 odst. 2 zákoníku práce²⁴⁹.

Byl(a) jsem poučen(a) o svém právu na informace o zpracování mých osobních údajů podle ustanovení § 12 zákona, jakož i o svých právech daných mi ustanovením § 21 (tj. *požádat správce o vysvětlení, když zjistím nebo se budu domnívat, že správce zpracovává mé osobní údaje v rozporu s ochranou mého soukromého a osobního života nebo v rozporu se zákonem. Jsou-li mé osobní údaje nepřesné s ohledem na účel jejich zpracování, mohu požadovat, aby správce odstranil takto vzniklý stav, zejména se může jednat o blokování, opravu, doplnění nebo jejich likvidaci*). V případě nevyhovění správcem mám právo obrátit se přímo na Úřad pro ochranu osobních údajů.

Souhlasím s použitím své fotografie jako součásti mého osobního spisu a s případným umístěním fotografie v digitální formě v databázi ISSP a na identifikačním průkazu vydaným zaměstnavatelem, a to po celou dobu trvání pracovního poměru k zaměstnavateli. Dále souhlasím s tím, že zaměstnavateli budu poskytovat aktuální osobní údaje a jejich změny.

²⁴⁹ *Do osobního spisu mohou nahlížet vedoucí zaměstnanci, kteří jsou zaměstnanci nadřizení. Právo nahlížet do osobního spisu má orgán inspekce práce, Úřad práce České republiky, Úřad pro ochranu osobních údajů, soud, státní zástupce, policejní orgán, Národní bezpečnostní úřad a zpravodajské služby. Za nahlížení do osobního spisu se nepovažuje předložení jednotlivé písemnosti zaměstnavatelem z tohoto spisu vnějšímu kontrolnímu orgánu, který provádí kontrolu u zaměstnavatele a který si tuto písemnost vyžádal v souvislosti s předmětem kontroly prováděné u zaměstnavatele.*

8.6 Příloha F Souhlas s využitím kontaktních údajů o.z. před nabytím účinnosti Obecného nařízení 2016/679²⁵⁰

Souhlas s využitím kontaktních údajů zaměstnance

pro pan(i)

Souhlasím se zpracováním svých osobních údajů – **kontaktních údajů** odbornými orgány zaměstnavatele – organizační složky státu Ministerstva obrany, které jsou součástí osobního dotazníku, v osobním spise, za účelem kontaktování mé osoby v mimopracovní době, a to po dobu trvání pracovně právního vztahu k zaměstnavateli.

V dne

.....
podpis zaměstnance

²⁵⁰ Formulář z Informačního systému o službě a personálu.

8.7 Příloha G Souhlas se zpracováním osobních údajů po skončení pracovního poměru o.z. před nabytím účinnosti Obecného nařízení 2016/679²⁵¹

Souhlas se zpracováním osobních údajů po skončení pracovního poměru

pro pan(i)

Souhlasím se zpracováním svých osobních údajů zaměstnavatelem nebo jinou právnickou osobou jako smluvním partnerem zaměstnavatele i po skončení pracovního poměru v rozsahu nezbytném k vypořádání vzájemných práv a povinností i s opatřeními zaměstnavatele k archivaci osobních údajů o mně vedených v rezortním správním archivu, kde mi budou na požádání předloženy k nahlédnutí nebo mi z nich budou za podmínek stanovených obecně závaznými pravidly pořízeny výpisy (opisy, kopie).

V dne

.....
podpis zaměstnance

²⁵¹ Formulář z Informačního systému o službě a personálu.

8.8 Příloha H Poučení o zpracování osobních údajů o.z. po nabytí účinnosti Obecného nařízení 2016/679²⁵²

Informace o zpracování osobních údajů

pro pan(i)

podle čl. 13 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „nařízení“).

Prohlašuji, že jsem byl(a) poučen(a) o tom, že osobní údaje, které jsem poskytl(a) v osobním dotazníku, jsou (budou) zpracovávány odbornými orgány zaměstnavatele – České republiky – Ministerstva obrany, Tychonova 221/1, Praha 6, IČO: 60162694, v rozsahu a pro účel vyplývající z těchto právních předpisů:²⁵³

- zákon č. 48/1997 Sb., o veřejném zdravotním pojištění a o změně a doplnění některých souvisejících zákonů;
- zákon č. 155/1995 Sb., o důchodovém pojištění;
- zákon č. 187/2006, o nemocenském pojištění;
- zákon č. 219/1999 Sb., o ozbrojených silách České republiky;
- zákon č. 222/1999 Sb., o zajišťování obrany České republiky;
- zákon č. 262/2006 Sb., zákoník práce;
- zákon č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy;
- zákon č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů;
- zákon č. 373/2011 Sb., o specifických zdravotních službách;
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti;
- zákon č. 582/1991 Sb. o organizaci a provádění sociálního zabezpečení;
- zákon č. 586/1992 Sb. o daních z příjmu;
- nařízení vlády č. 590/2006 Sb., kterým se stanoví okruh a rozsah jiných důležitých osobních překážek v práci;
- nařízení vlády č. 341/2017 Sb., o platových poměrech zaměstnanců ve veřejných službách a správě;
- vyhláška MF č. 114/2002 Sb., o fondu kulturních a sociálních potřeb.

²⁵² Formulář z Informačního systému o službě a personálu.

²⁵³ Ve znění pozdějších předpisů.

V rámci zaměstnavatele je zřízena pozice pověřence pro ochranu osobních údajů. Kontakt Mgr. Lucie Kazdová, adresa Ministerstvo obrany – 2015, nám. Svobody 471/4, 160 01 Praha 6, tel. 973 229 328.

Poskytnuté osobní údaje bude v souvislosti s pracovně právním vztahem soustřeďovat a vést personalista organizačního celku, u kterého budu (jsem) zařazen (a) a příslušný orgán ekonomické služby zaměstnavatele. Osobní údaje jsou vedeny v listinné podobě na formulářích, které jsem dobrovolně vyplnil(a) v souvislosti s uzavřením pracovně právního vztahu. Na jejich základě budou zároveň vedeny v elektronické podobě v Integrovaném subsystému o službě a personálu. Moje osobní údaje budou zpřístupněny odborným orgánům zaměstnavatele při plnění povinností podle výše uvedených právních předpisů, a to včetně zpracování v dalších informačních systémech zaměstnavatele, a mohou být zpřístupněny vedoucím zaměstnancům, kteří mi jsou (budou) nadřizeni a dalším osobám stanoveným v ustanovení § 312 odst. 2 zákoníku práce. V rámci poskytování služeb zabezpečení provozu informačních systémů zaměstnavatele mohou být předány moje osobní údaje ke zpracování poskytovatelům těchto služeb. Tito poskytovatele budou vždy smluvně vázáni k dodržování ochrany osobních údajů v souladu s nařízením. Mé osobní údaje budou jiným správcům předávány výhradně v rámci plnění povinností vyplývajících z výše uvedených právních předpisů a v souladu s nařízením.

Dále jsem byl informován o zpracování osobního údaje – fotografie za účelem jejího umístění na identifikačním průkazu vydaném Českou republikou – Ministerstvem obrany z důvodu kontroly nad vstupem osob do prostor zaměstnavatele a s tím spojené ochrany majetku, a za účelem zařazení do personální evidence zaměstnavatele z důvodu ztotožnění zaměstnance ze strany personalisty, a to po celou dobu trvání pracovněprávního vztahu.

Osobní údaje budou zpracovávány po dobu mého základního pracovněprávního vztahu a následně budou uloženy v archivu.

Byl(a) jsem poučen(a) o svém právu na informace o zpracovávání mých osobních údajů. Tím se v souladu s čl. 15 a 16 nařízení rozumí zejména právo na informace o účelu zpracování, totožnosti správce a jeho oprávněných zájmech a o příjemcích údajů a právu na opravu nepřesně vedených údajů. Současně jsem byl(a) poučen(a), že uvedené údaje jsou zpracovávány na základě zákonné povinnosti a nelze na ně uplatnit právo podle čl. 17 (právo na výmaz) a čl. 20 (přenositelnost údajů). Kdykoliv mám právo vznést podle čl. 21 nařízení námitku proti zpracování výše uvedených osobních údajů. V případě nevyhovění správcem mám právo obrátit se přímo na Úřad pro ochranu osobních údajů.

V dne

.....
podpis zaměstnance

8.9 Příloha I Souhlas se zpřístupněním osobních údajů nad rámec zákonného povolení po nabytí účinnosti Obecného nařízení 2016/679²⁵⁴

Souhlas

V souladu s čl. 6 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů dávám souhlas k tomu, aby osobní údaje o mně vedené v personální evidenci (uvést název organizačního celku) byly zpřístupněny (komu) za účelem (uvést účel zpracování), a to v tomto rozsahu (uvést rozsah např. – viz dále:)

- nahlížení do osobního spisu;
- pořízení kopie pracovní smlouvy a všech jejích dodatků a změn a jejich předání novému zaměstnavateli při přechodu práv a povinností z pracovněprávních vztahů;
- pořízení kopie zápočtu doby odborné praxe a popisu pracovního místa a jejich předání novému zaměstnavateli při přechodu práv a povinností z pracovněprávních vztahů;
- pořízení kopie posledního platového výměru a jejich předání novému zaměstnavateli při přechodu práv a povinností z pracovněprávních vztahů;
- poskytnutí osobních údajů pro splnění ohlašovací povinnosti pro Registr pojištěnců zdravotního a sociálního pojištění novým zaměstnavatelem při přechodu práv a povinností z pracovněprávních vztahů.

Souhlas se zpracováním výše uvedených osobních údajů vydávám na období

oddo

Vdne.....

Příjmení a jméno osoby vydávající souhlas:

Podpis osoby vydávající souhlas:

²⁵⁴ Formulář z Informačního systému o službě a personálu.

8.10 Příloha J Souhlas se zpracováním osobních údajů po skončení pracovního poměru o.z. po nabytí účinnosti Obecného nařízení 2016/679²⁵⁵

Informace pro zaměstnance

V souladu s čl. 5 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „nařízení“), Vás informuji o tom, že po ukončení Vašeho zaměstnání ubudou Vaše osobní údaje dále zpracovávány Oddělením péče o vojenské důchodce, a to za účelem zabezpečení jednotného postupu při realizaci péče o vojenské důchodce, tj. o vojáky a občanské zaměstnance anebo státní zaměstnance a zaměstnance ve služebních úřadech a v MO, kteří odcházejí do starobního důchodu nebo invalidního důchodu pro invaliditu 3. stupně ve smyslu § 3 odst. 3 vyhlášky MF č. 114/2002 Sb., o fondu kulturních a sociálních potřeb ve znění pozdějších předpisů, a splňují tak podmínky pro poskytování plnění z fondu kulturních a sociálních potřeb Ministerstva obrany. Jedná se o osobní údaje v tomto rozsahu:

- jméno, příjmení
- datum narození
- trvalé bydliště
- datum ukončení služebního poměru VZP
- datum ukončení služebního poměru státního zaměstnance
- datum ukončení pracovního poměru
- telefon, email
- datum přiznání starobního nebo invalidního důchodu pro invaliditu 3. stupně

V rámci poskytování služeb zabezpečení provozu informačních systémů zaměstnavatele mohou být předány moje osobní údaje ke zpracování poskytovatelům těchto služeb. Tito poskytovatele budou vždy smluvně vázáni k dodržování ochrany osobních údajů v souladu s nařízením. Mé osobní údaje budou jiným správcům předávány výhradně v rámci plnění povinností vyplývajících z výše uvedených právních předpisů a v souladu s nařízením.

Osobní údaje budou zpracovávány po dobu mého nároku na čerpání výhod podle uvedeného právního předpisu a následně budou uloženy v archivu.

Byl(a) jsem poučen(a) o svém právu na informace o zpracovávání mých osobních údajů. Tím se v souladu s čl. 15 a 16 nařízení rozumí zejména právo na informace o účelu zpracování, totožnosti správce a jeho oprávněných zájmech a o příjemcích údajů a právu

²⁵⁵ Formulář z Informačního systému o službě a personálu.

na opravu nepřesně vedených údajů. Současně jsem byl(a) poučen(a), že uvedené údaje jsou zpracovávány na základě zákonné povinnosti a nelze na ně uplatnit právo podle čl. 17 (právo na výmaz) a čl. 20 (přenositelnost údajů). Kdykoliv mám právo vznést podle čl. 21 nařízení námitku proti zpracování výše uvedených osobních údajů. V případě nevyhovění správcem mám právo obrátit se přímo na Úřad pro ochranu osobních údajů.

Vdne.....

Příjmení a jméno zaměstnance:

Podpis zaměstnance:

Podpis osoby ověřující výše uvedené údaje:

8.11 Příloha K Otázky pro řízený rozhovor

1. Jaké je Vaše služební zařazení v Armádě ČR?
2. Jak dlouho v rámci svého služebního zařazení zpracováváte osobní údaje fyzických osob?
3. Pro potřeby jaké agendy zpracováváte osobní údaje?
4. Na základě jakého pověření zpracováváte osobní údaje fyzických osob? Svoji odpověď rozveďte
 - a) na základě zákona
 - b) na základě jiného pověření
5. Jak hodnotíte své znalosti zákona č. 110/2019 Sb., o zpracování osobních údajů (příp. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „Obecné nařízení 2016/679“)?
 - a) úplné
 - b) částečné
 - c) žádné
6. V čem spatřujete své mezery v oblasti znalostí zákona č. 110/2019 Sb., o zpracování osobních údajů (popř. Obecného nařízení 2016/679)?
7. Jaké vidíte možné řešení k odstranění svých znalostních mezer?
8. Jaká technická a organizační opatření používáte k zabezpečení ochrany osobních údajů fyzických osob (ochrana proti neoprávněnému přístupu, zničení, změně, ztrátě či zneužití osobních údajů)?
9. Setkal/a jste se při zpracovávání osobních údajů fyzických osob se žádostí o likvidaci údajů, u kterých pominul účel zpracování?
10. V čem spatřujete základní rozdíl při zpracování osobních údajů v ČR před a po nabytí platnosti Obecného nařízení 2016/679?
11. Přinesla aplikace Obecného nařízení 2016/679 zvýšené požadavky a nároky na Vaši činnost v Armádě ČR? Vyberte z nabízených možností (může jich být více) a blíže specifikujte:
 - a) administrativní
 - b) ekonomické
 - c) časové
 - d) žádné
 - e) jiné (uved'te)

Který v případě více uvedených dopadů Obecného nařízení 2016/679 na Vaši činnost považujete za nejvýraznější?
12. Jak hodnotíte nabytí platnosti Obecného nařízení 2016/679? Svoji odpověď rozveďte ve smyslu, proč ji takto hodnotíte?
 - a) zcela pozitivně

- b) spíše pozitivně
 - c) spíše negativně
 - d) zcela negativně
 - e) zatím nemohu posoudit
13. Setkal/a jste se s problémy při zpracování osobních údajů s ohledem na Armádu ČR, které Obecné nařízení 2016/679 nezohledňuje?
14. Myslíte, že Obecné nařízení 2016/679 přispívá k řešení rizik spojených s širokým užíváním sociálních sítí? Jaké problémy, v souvislosti s užíváním sociálních sítí, vidíte v Armádě ČR?