POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostního managementu

Katedra veřejného práva

Ochrana osobních údajů vykonávaná orgánem státní správy

Diplomová práce

The Protection of personal data performed by a state administration body

Diploma thesis

VEDOUCÍ PRÁCE
doc. JUDr. Jan Tryzna, Ph.D.

AUTOR PRÁCE
Bc. Jaroslav Mach, DiS.

PRAHA
2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, který jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne

.....
Jaroslav Mach

Poděkování

Děkuji vedoucímu diplomové práce doc. JUDr. Janu Tryznovi, Ph.D. za cenné rady, připomínky a metodické vedení práce. Dále bych rád poděkoval mým kolegům za jejich odborná vyjádření a další postřehy k dané problematice. Zároveň bych rád poděkoval i své rodině za trpělivost a morální podporu, kterou mi po celou dobu studia věnovali.

Anotace

Tato diplomová práce se zabývá institucionálními aspekty ochrany osobních údajů v orgánech státní správy. V rámci toho vymezuje předmětnou legislativu a pojmosloví, charakterizuje státní správu, analyzuje potřeby kladené právními normami v každodenních činnostech těchto orgánů, včetně postupů realizovaných státním dozorovým úřadem ve vztahu k ochraně osobních údajů. Práce také pojednává o informační bezpečnosti, která tvoří nedílnou součást při zajištění ochrany osobních údajů v uvedených orgánech. V návaznosti na to zmiňuje některé prvky kybernetické bezpečnosti. Výsledkem je tak ucelený přehled pojednávající z vícera aspektů o problematice ochrany osobních údajů v institucionálním sektoru státní správy.

Klíčová slova

Legislativa, státní správa, ochrana osobních údajů, kamerové systémy, informační bezpečnost, kybernetická bezpečnost

Annotation

This diploma thesis deals with institutional aspects of personal data protection in state administration bodies. As part of this, it defines the relevant legislation and terminology, characterizes the state administration, analyzes the needs imposed by legal standards in the day-to-day activities of these bodies, including the procedures implemented by the state supervisory authority in relation to the protection of personal data. The thesis also deals with information security, which forms an integral part in ensuring the protection of personal data in the mentioned authorities. Following this, it mentions some elements of cybersecurity. The result is a comprehensive overview of several aspects of the issue of personal data protection in the institutional sector of state administration.

Key words

Legislation, state administration, personal data protection, camera systems, information security, cybersecurity

Obsah

1 Úvod 7
2 Legislativní vymezení 10
3 Státní správa 15
4 Ochrana osobních údajů 19
4.1 Základní pojmy 19
4.2 Práva a povinnosti 24
4.2.1 Správce 24
4.2.2 Zpracovatel 30
4.2.3 Subjekt údajů 33
4.2.4 Základní zásady zpracování 42
4.2.5 Pověřenec 45
4.2.6 Sbor pověřenců 46
4.2.7 Zabezpečení osobních údajů 47
4.2.8 Porušení zabezpečení osobních údajů 48
4.3 Vnitropodniková dokumentace 49
4.3.1 Vnitřní předpis 50
4.3.2 Záznamy o činnostech zpracování 50
4.3.3 Technická a organizační opatření 52
4.3.4 Posouzení rizika 54
4.3.5 Posouzení vlivu a balanční test 56
4.3.6 Diferenciace dokumentace 57
4.4 COVID-19 58
4.5 Kamerový systém 59
4.6 Úřad pro ochranu osobních údajů 68
4.6.1 Konzultační činnost 69
4.6.2 Dozorová činnost 70

5 Informační a kybernetická bezpečnost 71
5.1 ISO normy 76
6 Závěr 77
7 Seznam použité literatury 79
7.1 Monografie 79
7.2 Zákonná úprava a interní akty řízení 80
7.3 Webové stránky a elektronické zdroje 83

1 Úvod

Ochrana osobních údajů je oblast, která s rozvojem digitální techniky a jejím šířením napříč celou společností vyžaduje čím dál větší pozornost, včetně vyšších nároků na zabezpečení dat, ve kterých jsou tyto informace obsaženy. Téma ochrany osobních údajů rezonovalo společností zejména v roce 2018, kdy vešlo v účinnost nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Nařízení vešlo v platnost již v roce 2016, kdy bylo uveřejněno v Úředním věstníku Evropské unie. Zákonodárcem Evropské unie, za kterého je nejčastěji považován Evropský parlament a Rada Evropské unie[1], byl však ponechán prostor, aby státní i soukromé instituce mohly uvést obecné nařízení o ochraně osobních údajů do souladu se svou předpisovou základnou a aplikovat ho v příslušných procesech. To platilo jak pro zákonodárce členských států Evropské unie (dále jen „EU“) v oblasti případných změn některých vnitrostátních právních norem, anebo doplnění o nové, tak i pro podniky a instituce, které musely nařízení implementovat do své vnitropodnikové dokumentace a seznámit s ním své vedení a zaměstnance. Nezřídka kdy se však ukázalo, že ani tento poměrně dlouhý čas nestačil k tomu, aby veřejný i soukromý sektor dostatečně zajistily jak odborné vedení při implementaci všech opatření, potažmo odborné pracovníky, tak příslušnou dokumentaci. Samotná povinnost řádného zpracování osobních údajů tu ovšem byla již dlouhou dobu předtím (viz kapitola č. 2 „Legislativní vymezení“).

Samotná potřeba chránit osobní údaje však nepřichází jen s rozvojem digitální techniky. Obecně rozvoj technologií přispěl ke globalizaci, kdy osobní údaje lidí z jedné části světa mohou být v krátké chvíli zaznamenávány a zpracovávány mimo území státu, ve kterém tato osoba či skupiny osob žijí, čímž se riziko ohrožení soukromí osob zvyšuje. Stejně tak tyto údaje mohou být zpracovávány v tzv. třetích zemích, tedy mimo EU. Zde je pak nutné zajistit, aby úroveň

[1] Fáze legislativního procesu v EU - Euroskop. *Hlavní strana - Euroskop* [online]. Copyright © 2005 [cit. 20.07.2022]. Dostupné z: https://euroskop.cz/evropska-unie/rozhodovani-eu/faze-legislativniho-procesu-v-eu/

ochrany osobních údajů předávaných do těchto zemí byla na stejné nebo vyšší úrovni, než jakou poskytuje právo EU. Poměrně častým úkazem dnešní doby je totiž snaha získávat osobní údaje a obchodovat s nimi, nejčastěji za účelem finančního zisku nebo za účelem získání informací o osobách, které mohou posloužit k jinému neoprávněnému zpracování, a tím k dalšímu z toho plynoucímu profitu.

Právě výše uvedené faktory přispěly k tomu, že došlo k diskusi o potřebě právní úpravy, která bude reflektovat jak současný technologický pokrok, tak potřebu zajistit ochranu fyzických osob, aby nedocházelo k situacím, kdy budou využity nebo zneužity osobní údaje pro účely, které nejsou jejich původci známy. Rovněž se přistoupilo k tomu, že nová právní úprava bude přímo závazná a použitelná pro všechny členské státy EU a nebude na bázi určité dobrovolnosti, jako tomu je u vydávaných směrnic. Pro zajištění dostatečné vážnosti a důležitosti je toto úsilí podpořeno také poměrně vysokými sankcemi, které mohou být uděleny při porušení povinností vycházejících z již zmíněného obecného nařízení o ochraně osobních údajů, které je známé také pod zkratkou „*GDPR*“, což označuje anglické sousloví „*General Data Protection Regulation*“. Kromě toho se při neoprávněném nakládání s osobními údaji může osoba disponující či manipulující s těmito údaji vystavovat také hrozbě trestního stíhání podle ust. § 180 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a dále také například dle § 182, § 183 nebo § 230 tamtéž.

V rámci některých požadavků, které GDPR přineslo, se zvýšily také požadavky na státní orgány, zejména v oblasti informační bezpečnosti. Tlak vyvíjený na digitalizaci státní správy klade stále větší důraz na efektivní a kvalitní zpracování informací a dat, což souvisí s investicemi do technologií a obnovy zastaralé techniky. Státní orgány tak musely začít posuzovat, zda jejich nastavené procesy odpovídají novým potřebám a v této souvislosti zavádět často prvky, které do té doby nebyly uvažovány, anebo na ně nebyla vůle uvolnit finanční prostředky, nejčastěji z důvodu omezování investičních nákladů. Jedná se však o oblast poměrně dynamickou, ve které je nutné ruku v ruce s rozvojem technologií dbát na zajištění právního rámce a příslušné implementace opatření. Není proto

možné tuto agendu brát na lehkou váhu, ale naopak zajistit, aby její správné nastavení pomáhalo příslušným institucím usnadnit reagovat na budoucí změny.

Práce se zaměřuje na požadavky kladené legislativou, místy se prolínají jednotlivá práva a povinnosti dotčených subjektů, jelikož někdy ani není možné tyto vztahy od sebe zcela separovat. Kapitoly jsou zaměřeny na normativní i technické aspekty ochrany osobních údajů, se snahou o jejich propojení, a tím také o jednotnou, ale nikoli úplnou standardizaci obecných postupů při plnění aktivit v této oblasti. Cílem je zejména analyzovat problematiku v této rozvíjející se oblasti ve vztahu k orgánům státní správy, dále pak přiblížit výkon státní správy v oblasti ochrany osobních údajů, zaměřit se na téma informační bezpečnosti a deduktivním i komparativním přístupem prezentovat různá specifika, která jsou pro zmíněné instituce typická.

2 Legislativní vymezení

Přestože byl rok 2018 do jisté míry pro ochranu osobních údajů přelomový, nejednalo se o zcela nový právní instrument, který by zaváděl ochranu osobních údajů jako novum. V České republice za prvotní, avšak nikoli zcela ucelený právní předpis, lze považovat zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který však neupravoval zpracování osobních údajů v listinné podobě, stejně tak nezřizoval ani dozorový úřad. Nejcitelněji byla ochrana osobních údajů v právním řádu České republiky zakotvena až zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „ZoOOÚ"), který více reflektoval změny ve společnosti a potřebu nastavení některých prvků, které do té doby v zákonných normách chyběly. Tento zákon nahradil právní předpis z roku 1992 a v průběhu času byl několikrát novelizován. Oproti původnímu zákonu byl podstatně komplexnější. Vymezil potřebné pojmy, stanovil práva a povinnosti osob, včetně přestupků při jejich porušení. Umožnil zřízení dozorového úřadu, kterým je Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ") a více dbal na zpracování osobních údajů v evidencích. Zároveň bylo nutné před vstupem České republiky do Evropské unie přijmout v této oblasti odpovídající normativní právní akt, který položí základní kámen pro budoucí aplikaci norem komunitárního práva působícího na území členských států. Komunitárním právem se rozumí „*směrnice, nařízení, rozhodnutí přijatá na základě Smluv a další prameny práva, které tvoří dohromady primární právo Evropské unie a Společenství*"[2].

V souvislosti s připravovaným a později uskutečněným vstupem České republiky do EU prošel ZoOOÚ významnou novelizací, která měla za cíl transponovat do českého právního řádu směrnici 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 (dále jen „Směrnice 95/46/ES"). Tato směrnice navazovala na Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat (vyhlášená pod č. 115/2001 Sb. m. s.).

[2] Slovníček pojmů - Komunitární právo - BusinessCenter.cz. *BusinessCenter.cz* [online]. Copyright © 1997 [cit. 20.07.2022]. Dostupné z: https://businesscenter.podnikatel.cz/slovnicek/komunitarni-pravo/

Úmluva č. 108, jak bývá zkráceně označována, byla přijata již v roce 1981 a Českou republikou ratifikována v roce 2001. Definovala některé důležité pojmy, stanovila zvláštní skupiny údajů, určila zásady zpracování a větší nutnost zabezpečení pro tyto údaje. Později byla doplněna Směrnicí 95/46/ES, která více reagovala na potřeby moderní doby a soudobé praxe (kupříkladu se přestalo oddělovat automatizované a neautomatizované zpracování osobních údajů a zvýšila se ochrana soukromí osob).

S postupem času a s ohledem na neustálý posun k informační společnosti docházelo k diskusi o změně Směrnice 95/46/ES na nařízení, které by směrnici nahradilo a v některých bodech rozšířilo. Zároveň mělo jít o právně závazný a přímo aplikovatelný předpis pro všechny členské státy EU, platný na celém jejím území, aby došlo k jednotné harmonizaci právního aktu bez možnosti extenzivního výkladu, jak tomu mnohdy bylo u Směrnice 95/46/ES.

Toho bylo docíleno přijetím nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), které nahradilo ZoOOÚ, jelikož je také přímo aplikovatelnou normou bez nutnosti její transpozice do právního řádu členského státu. K takové normě však bývá většinou doprovodný adaptační zákon, který upravuje některé procesní záležitosti. Tím je v České republice zákon č. 110/2019 Sb., o zpracování osobních údajů (dále jen „ZoZOÚ“), který definitivně zrušil do té doby ještě platný ZoOOÚ.

Tento adaptační (či také prováděcí) zákon se bohužel nestihl přijmout do data účinnosti obecného nařízení o ochraně osobních údajů (dále jen „Obecné nařízení“), což znamenalo problémy při řešení některých postupů. Adaptačním zákonem, jímž měl být právě ZoZOÚ, se měla upravit některá pravidla, u nichž Obecné nařízení ponechává členským státům prostor pro korekci. Uvedený předpis upravuje působnost ÚOOÚ, dále některé přestupky, a zároveň implementuje Směrnici 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 (dále jen „Směrnice 2016/680“), někdy též nazývána jako trestněprávní směrnice, která se vztahuje na zpracování osobních údajů při činnostech v oblasti justiční spolupráce v trestních věcech a policejní spolupráce. Pro výkon orgánu státní správy ve většině případů není nutné tuto trestněprávní směrnici aplikovat, nejedná-li se o orgán, který by s těmito informacemi přímo nakládal, a není proto ani součástí dalšího obsahu této práce.

Ochrana osobních údajů je také reflektována v ústavním pořádku České republiky, konkrétněji v Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky (dále jen „Listina ZPS“). Zde se v čl. 7 odst. 1 uvádí: „*Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.*“ Dále pak v čl. 10 odst. 2 Listiny ZPS: „*Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.*“, a také v čl. 10 odst. 3 Listiny ZPS: „*Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.*“ Za případné povšimnutí stojí, že přijetí zákona z roku 1992 (platnost od 01.06.1992, účinnost od 01.06.1992) předběhlo přijetí Listiny ZPS (platnost od 28.12.1992, účinnost od 01.01.1993).

Mimo výše uvedený výčet je možné zmínit i další zákony, které v určité míře upravují ochranu osobních údajů. Ze soukromoprávního hlediska lze uvést například ust. § 77 až § 114 zákona č. 89/2012 Sb., občanský zákoník, upravující jméno a bydliště člověka (ust. § 77 až § 80) a ochranu osobnosti člověka (ust. § 81 až § 114). Z veřejnoprávního hlediska má nejsilnější pozici ust. § 180 zákona č. 40/2009 Sb., trestní zákoník, ve kterém se postihuje neoprávněné nakládání s osobními údaji, včetně sankcí v podobě uložení peněžitého trestu, zákazu činnosti nebo odnětí svobody. Mezi další předpisy a příklady některých ustanovení je možné zařadit ust. § 87 až 88 a ust. § 95 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých

souvisejících zákonů (zákon o elektronických komunikacích) nebo ust. § 22c zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Zákon o kybernetické bezpečnosti je však provázán s ochranou osobních údajů podstatně více (viz kapitola č. 5 „Informační bezpečnost“). Důležité jsou také zákony upravující provoz informačních systémů a registrů veřejné správy. Pro příklad zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, nebo zákon č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob.

Zásadní je zde také dodat, že ochrana osobních údajů bývá provedena různými zvláštními zákony a prováděcími právními předpisy, a to jak evropskými, tak českými, přestože většina z nich již koresponduje právě s podmínkami kladenými evropskou legislativou, případně v rámci novelizací dochází k jejich souladu. Výčet právních předpisů uvedených v této práci proto nelze brát za výčet celkový, ale spíše orientační, včetně uvedených ustanovení jednotlivých zákonů. Příklady některých dalších právních dokumentů jsou uvedeny níže.

Evropské právní dokumenty:

- Listina základních práv Evropské unie (článek 8)
- Smlouva o fungování Evropské unie (článek 16)
- Dodatkový protokol k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice (vyhlášený pod č. 29/2005 Sb. m. s.)
- Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Text s významem pro EHP)
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)

- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) - tato směrnice byla změněna Směrnicí Evropského parlamentu a rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES, o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004, o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele
- Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích

Právní dokumenty České republiky:

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- zákon č. 111/2009 Sb., o základních registrech
- zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů
- zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel)
- zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)
- zákon č. 159/2006 Sb., o střetu zájmů
- zákon č. 262/2006 Sb., zákoník práce
- zákon č. 273/2008 Sb., o Policii České republiky
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)

3 Státní správa

Státní správa je součástí systému veřejné správy, kterou členíme na dva subsystémy, a to na státní správu a samosprávu, někdy též nazývanou jako územní samosprávu. Z pohledu státní moci patří do moci výkonné (tj. realizuje výkonnou moc státu), která je zakotvena v hlavě třetí Ústavy České republiky[3] (dále jen „Ústava"). Vykonávají ji orgány veřejné moci, kterými v případě „*přímého*"[4] výkonu státní správy jsou orgány státu jako vláda (vrcholný orgán výkonné moci podle čl. 67 odst. 1 Ústavy), ministerstva a další správní úřady, a při „*nepřímém*"[5] výkonu státní správy pak obecní nebo krajské úřady územních samosprávných celků (obcí, krajů), které vykonávají tuto činnost v přenesené působnosti. Územní samosprávu vymezuje hlava sedmá Ústavy, kde je v čl. 105 uvedeno, že „*Výkon státní správy lze svěřit orgánům samosprávy jen tehdy, stanoví-li to zákon.*" Příkladem přenesené působnosti může být například povolování staveb ve stavebním řízení nebo vydávání občanských a řidičských průkazů. V tomto případě se mluví o decentralizaci státní moci na veřejnoprávní korporace, které jsou zřizovány zákonem a jsou zároveň subjektem veřejného práva. Vhodné v tomto ohledu je ještě doplnit, že na základě ust. § 92 zákona č. 129/2000 Sb., o krajích (krajské zřízení), jsou při výkonu přenesené působnosti orgány územní samosprávy podřízeny příslušnému ministerstvu. Jednotlivá ministerstva následně řídí v oblastech svých agend přenášených na orgány územní samosprávy výkon státní správy vydáváním směrnic a vyhlášek[6].

Z výše uvedeného plyne také další charakteristika státní správy. Ta je oproti správě soukromé z mnohem větší části regulována právem, z čehož pramení podstatně větší vázanost právním řádem. Rovněž zasahuje častěji do veřejných záležitostí a veřejného života každého občana v daném státě, k čemuž je vybavena státní mocí, kterou uplatňují již zmíněné orgány veřejné moci (dále jen „OVM"). Státní moc, která spadá pod veřejnou moc, je mocí projevovanou státními orgány, kdy nositelem moci je stát. Veřejnou moc definuje například

[3] Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších ústavních zákonů
[4] BŘEŇ, J., Základní charakteristika státní správy. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu), s. 40-41.
[5] Tamtéž, s. 40-41.
[6] Tamtéž, s. 43

usnesení ústavního soudu z roku 1993[7], které uvádí, že „*Veřejnou mocí se rozumí taková moc, která autoritativně rozhoduje o právech a povinnostech subjektů, ať již přímo, nebo zprostředkovaně. Subjekt, o jehož právech nebo povinnostech rozhoduje orgán veřejné moci, není v rovnoprávném postavení s tímto orgánem a obsah rozhodnutí tohoto orgánu nezávisí od vůle subjektu.*“ Obecně lze tedy vymezit OVM jako orgány moci zákonodárné, výkonné a soudní, spolu s orgány územní samosprávy[8], popřípadě jako orgány, které reprezentují veřejnou moc a jsou ze zákona oprávněny autoritativně rozhodovat o právech a povinnostech fyzických či právnických osob nebo jinak zasahovat do jejich právní sféry, a to buď přímo (orgány moci výkonné a soudní) nebo zprostředkovaně (orgány moci zákonodárné)[9]. Co do zákonného vymezení lze nalézt definici v ust. § 2 písm. c) zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů. Tato definice je však sporná[10].

Státní správu je možné také dělit na *ústřední* a *územní*[11]. Ústřední státní správou jsou ministerstva a jiné ústřední správní úřady (dále také jako „státní instituce“), které mají celostátní působnost. Ministerstva a jiné správní úřady lze zřídit a jejich působnost stanovit pouze zákonem, jak vyplývá z čl. 79 odst. 1 Ústavy. Tyto úřady jsou ustanoveny tzv. kompetenčním zákonem, tedy zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů. Výčet ministerstev je uveden v ust. § 1 tohoto zákona. Výčet ústředních správních úřadů pak v ust. § 2, mezi

---

[7] Usnesení Ústavního soudu ze dne 25. 11. 1993 sp. zn. II. ÚS 75/93. NALUS - databáze rozhodnutí Ústavního soudu. *Charekteristika veřejné moci* [online]. [cit. 22.07.2022]. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=2-75-93

[8] Orgány veřejné moci v ČR | Ústav státu a práva Akademie věd České republiky. *Ústav státu a práva Akademie věd České republiky* [online]. Copyright © 2022 ÚSP [cit. 22.07.2022]. Dostupné z: https://www.ilaw.cas.cz/vyzkum/ceske-pravo-informace-a-odkazy/organy-verejne-moci-v-cr.html

[9] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 111.

[10] K vymezení a aplikaci pojmu „orgán veřejné moci“ podle zákona o základních registrech - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2022 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 22.07.2022]. Dostupné z: https://www.mvcr.cz/clanek/k-vymezeni-a-aplikaci-pojmu-organ-verejne-moci-podle-zakona-o-zakladnich-registrech.aspx

[11] BŘEŇ, J., Základní charakteristika státní správy. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu), s. 39-40, s. 60.

nimiž je uveden například Český statistický úřad, ale také Úřad pro ochranu osobních údajů nebo Národní úřad pro kybernetickou a informační bezpečnost. Územní státní správou jsou pak územní správní úřady s působností na území správního obvodu, okresu nebo kraje. Jedná se například o finanční nebo katastrální úřad, popř. úřad práce či obvodní báňský úřad. Jednotlivé druhy úřadů, stejně jako další instituce nebo organizace vykonávající činnost státní správy, lze nalézt i ve veřejně dostupných zdrojích[12].

Státní správa může být rovněž vykonávána „*vrchnostensky*" a „*nevrchnostensky*"[13]. V prvním případě se jedná o vztahy nadřízenosti a podřízenosti[14], kdy státní orgán autoritativně vystupuje vůči ostatním adresátům (něco nařizuje, o něčem rozhoduje), čímž zasahuje do jejich právních poměrů. V druhém případě jde o rovnoprávný vztah, kdy je při zajišťování (obhospodařování) určitých veřejných potřeb vstupováno do různých soukromoprávních vztahů (např. u přijímání zaměstnanců do pracovního poměru nebo při nakládání se státním majetkem). Státní správa je tedy veřejná správa uskutečňovaná státem, která má *výkonný*, *podzákonný* a *nařizovací* charakter, kdy výkonným charakterem je provádění (vykonávání) zákonů, podzákonným se rozumí činnost orgánů státní správy v mezích zákona (vázanost právním řádem) a nařizovacím pak uplatňování autority státních orgánů za pomoci různých mocenských nástrojů, které zajišťují vynutitelnost normativních správních aktů vůči jejich adresátům[15].

Z pohledu právních předpisů ovlivňujících výkon státní správy je možné zmínit např. zákon č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád). Dále pak např. zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů nebo zákon č. 499/2004

[12] Adresář úřadů - statnisprava.cz. *statnisprava.cz [online].* Copyright © Copyright 2000 [cit. 22.07.2022]. Dostupné z: https://www.statnisprava.cz/rstsp/ciselniky.nsf/druhy_uradu
[13] BŘEŇ, J., Základní charakteristika státní správy. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu), s. 34 - 35.
[14] Tamtéž, s. 43 - 44.
[15] Tamtéž, s. 43.

Sb., o archivnictví a spisové službě a o změně některých zákonů. Jako kontrolní prvek státní správy, ale i územní samosprávy, slouží kromě k tomu určených kontrolních orgánů a jiných právních předpisů také zákon č. 106/1999Sb., o svobodném přístupu k informacím (dále jen „zákon o svobodném přístupu k informacím“), ve znění pozdějších předpisů, který umožňuje veřejnosti získávat informace z výkonu činnosti těchto orgánů. Z logiky věci se však nejedná o informace podléhající určitému stupni utajení podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, anebo o jiné citlivé informace nepřísluší ke sdělení, případně sdělované pouze za určitých zákonem stanovených podmínek. Dalším tomu podobným předpisem je také zákon č. 123/1998 Sb., o právu na informace o životním prostředí.

Při poskytování informací veřejnosti je brán zřetel na povahu těchto informací. Proto se také v zákoně o svobodném přístupu k informacím v ust. § 7 uvádí: „*Je-li požadovaná informace v souladu s právními předpisy označena za utajovanou informaci, k níž žadatel nemá oprávněný přístup, povinný subjekt ji neposkytne.*“ Dále pak v ust. § 8a odst. 1: „*Informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu.*“ Tím zákonodárce pamatuje také na potřebu ochrany osobních údajů v této oblasti, jelikož není žádoucí, aby veškeré osobní údaje byly komukoliv a kdykoliv dostupné. Zároveň musí docházet k pseudonymizaci (viz kap. 4.3.3) poskytovaných údajů fyzických osob, aby nedocházelo k jejich neoprávněnému zpracování či zneužití. Určitou výjimku tvoří ust. § 8a odst. 2, kde je zmíněno, že: „*Povinný subjekt poskytne osobní údaje o veřejně činné osobě, funkcionáři nebo zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti nebo o jeho funkčním nebo pracovním zařazení.*“ Na základě tohoto ustanovení se mohou fyzické osoby dožadovat informací vztahující se k osobám v určitém postavení, tedy například vyžadovat informace spojené s jejich odměňováním[16].

[16] Informace k platům a odměnám | MPO. *Ministerstvo průmyslu a obchodu* [online]. Copyright © Copyright 2005 [cit. 06.08.2022]. Dostupné z: https://www.mpo.cz/cz/rozcestnik/ministerstvo/aplikace-zakona-c-106-1999-sb/informace-zverejnovane-podle-paragrafu-5-odstavec-3-zakona/informace-k-platum-a-odmenam--266205/

4 Ochrana osobních údajů

4.1 Základní pojmy

O problematice ochrany osobních údajů, její podstatě a potřebě zavedení některých souvisejících nástrojů již bylo částečně pohovořeno. V této návaznosti a pro další porozumění psaného textu, je nutné uvést alespoň některé základní pojmy, které se k předmětné oblasti vztahují. Níže jsou věcně definovány tak, jak vycházejí přímo z Obecného nařízení. Pro případné srovnání se mohou vyskytnout i některé pojmy ze ZoZOÚ, ZoOOÚ nebo judikatury, na což bude v takovém případě upozorněno. Uvedené pojmy nejsou komplexním vymezením všech pojmů, ale reflektují určitou potřebu seznámení se s nimi. Některé další pojmy budou podle potřeby upřesněny dále v textu. Pokud se hovoří o „recitálu", mají se na mysli jednotlivé číselně označené body v úvodním ustanovení Obecného nařízení, což lze v prostředí českého práva chápat také jako preambuli pojednávající o důvodech přijetí, významných hodnotách, potřebách a historickém kontextu Obecného nařízení.

Na začátek je potřeba si představit, co je **osobní údaj** a čím se vyznačuje. Osobními údaji, jak je definuje v čl. 4 odst. 1 Obecné nařízení, se rozumí „…*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů").*" Každý podnik či instituce, která je v roli správce osobních údajů, musí být schopna doložit subjektu údajů jaké osobní údaje o něm zpracovává. To je jeden ze záměrů, k jakým mělo Obecné nařízení docílit. Tento záměr lze označit termínem „*transparentnost*" uvedeným v čl. 12 tohoto nařízení.

Konkrétněji se pak osobním údajem v běžném kontaktu rozumí například jméno, věk (a s ním spojené datum narození), pohlaví, osobní stav (vdaná, rozvedený, svobodný), adresa místa bydliště, e-mailová adresa, osobní fotografie, telefonní číslo nebo IP adresa (IP adresou se rozumí „*Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti,…*")[17]. V rámci pracovního zařazení se pak

[17] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015.

může jednat o číslo k pracovnímu telefonu, pracovní email, adresa místa výkonu práce, pracovní identifikační číslo zaměstnance nebo přihlašovací uživatelské jméno či jiné ověřovací identifikační údaje. Další případné upřesnění pojmu osobní údaj lze nalézt v rozhodnutí Nejvyššího správního soudu pod spisovou značkou 9 As 34/2008-68. Zde je na str. 5 uvedeno, že *„…se výklad pojmu „osobní údaj“ nemůže omezit striktně jen na znalost např. rodného čísla, adresy či pracoviště subjektu údajů. Z tohoto pohledu je za osobní údaj třeba považovat i číslo mobilního telefonu určité osoby, jakkoli může být takové číslo používáno příslušnou osobou jen dočasně, a zároveň nijak nespecifikuje jeho fyzickou, psychickou, ekonomickou, kulturní nebo sociální identitu (…).*“

Subjektem údajů se pak podle čl. 4 odst. 1 Obecného nařízení rozumí *„…fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména s 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.*“ Obdobné vymezení uváděl také ZoOOÚ v ust. § 4 písm. a), kde docházelo pouze k lexikálním odchylkám. Pro lepší upřesnění definuje subjekt údajů také český zákonodárce, který přistoupil k vlastní definici v ust. § 3 ZoZOÚ, která je stejná jako v předchozí právní úpravě v ust. § 4 písm. d) ZoOOÚ. V obou případech se subjektem údajů rozumí fyzická osoba, k níž se osobní údaje vztahují. Pro zajímavost lze dodat, že subjektem údajů se má na mysli žijící fyzická osoba, nikoli osoba zesnulá. Při zpracování údajů se pak přistupuje zejména k právnímu titulu zpracování, jelikož souhlas subjektů údajů je s nástupem Obecného nařízení druhořadým právním titulem, nikoli primárním.

Kromě osobního údaje ještě rozeznáváme kategorii **citlivých údajů.** Citlivým údajem se rozumí tzv. zvláštní kategorie osobních údajů, která je více popsána v čl. 9 Obecného nařízení. Dále je zmíněna také v recitálu 10 Obecného nařízení, kde se uvádí, že *„Toto nařízení rovněž poskytuje členským státům určitý prostor ke stanovení vlastních pravidel, včetně pravidel pro zpracování zvláštních kategorií osobních údajů („citlivé osobní údaje“).“* V recitálu 51 Obecného nařízení se k čl. 9 uvádí: *„Osobní údaje, které jsou svou povahou*

obzvláště citlivé z hlediska základních práv a svobod, zasluhují zvláštní ochranu, jelikož by při jejich zpracování mohla vzniknout závažná rizika pro základní práva a svobody.“ Obdobně se toto uvádí také v recitálu 37 Směrnice 2016/680. Za citlivé osobní údaje se podle článku 9 Obecného nařízení považují *„osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.“* Tuto charakteristiku uváděl též ZoOOÚ v ust. § 4 písm. b). Novější ZoZOÚ někdy upřesňuje samotné zpracování těchto údajů, například v ust. § 16 odst. 2, anebo v ust. § 17 odst. 1, a samotný citlivý údaj pak definuje v ust. § 66 odst. 6, kde se ztotožňuje s Obecným nařízením.

Jednou z hlavních činností, kterou se správce (případně zpracovatel) zabývá, a subjekt údajů může v této věci žádat o informace či požadovat další úpravy a změny při nakládání se svými osobními údaji, je agenda či proces **zpracování** osobních údajů. Zpracováním osobních údajů se rozumí *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“* V obdobném duchu byla tato definice uvedena v ust. § 4 písm. e) ZoOOÚ, kde se zpracováním rozumí *„zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“*. Místy je užita jiná lexikální formulace vyjadřující co do smyslu stejný obsah. Podstata samotného zpracování je vyjádřena v recitálu 4 Obecného nařízení: *„Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy.“*, a dále také v recitálu 39 tamtéž.

Tím, kdo nese hlavní odpovědnost za zpracování osobních údajů a za jejich bezpečnost je **správce** osobních údajů. Správcem se podle čl. 4 odst. 7 Obecného nařízení 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.“*

V některých případech se může stát, že správce přistoupí k uzavření dohody se **zpracovatelem**, který pro něj v určité míře (menší či větší) osobní údaje zpracovává. Pravidla zpracování v takovém případě určuje správce, což ale neznamená, že se správce zbavuje odpovědnosti, kterou obrazně řečeno přenáší na zpracovatele. Faktickým zajišťovatelem bezpečnosti je stále správce. Zpracovatelem se rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.“* Povinnosti pro zpracovatele následně stanovuje Obecné nařízení v čl. 28, který je i základním východiskem pro uzavírání smluv. V ust. § 4 písm. k) ZoOOÚ byl zpracovatel definován jako *„subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona“*. Důležitým faktorem pro uzavření smlouvy se zpracovatelem je, že poskytuje dostatečné záruky bezpečnosti při zpracování získaných osobních údajů, a že má zavedena veškerá příslušná opatření, která jsou v souladu s Obecným nařízením.

V roce 2022 a zřejmě i v roce následujícím je poměrně stále ještě aktuální onemocnění COVID-19[18] (anglická zkratka pro coronavirus disease 2019). Na počátku roku 2020 se toto celosvětové onemocnění stalo pro zpracování osobních údajů leckde palčivým problémem, a to v souvislosti s povinným testováním zaměstnanců ve firmách, a následně i ve státních institucích. Tím byla také prověřena schopnost státních orgánů i ÚOOÚ reagovat na tuto situaci, což mnohdy nebylo snadné. **Údaji o zdravotním stavu** se podle čl. 4 odst. 15

[18] WHO Coronavirus (COVID-19) Dashboard | WHO Coronavirus (COVID-19) Dashboard With Vaccination Data. *WHO Coronavirus (COVID-19) Dashboard | WHO Coronavirus (COVID-19) Dashboard With Vaccination Data* [online]. [cit. 25.07.2022]. Dostupné z: https://covid19.who.int/

rozumí *„osobní údaje týkající se tělesného nebo duševního zdraví fyzické osoby, včetně údajů o poskytnutí zdravotních služeb, které vypovídají o jejím zdravotním stavu.“* Tyto údaje, jak již bylo zmíněno, řadíme mezi citlivé osobní údaje, a proto se k nim musí přistupovat se zvláštní obezřetností.

Níže jsou uvedeny některé další relevantní pojmy z Obecného nařízení již bez přidaného komentáře. Pro případné seznámení se s kompletním výčtem některých zbylých pojmů, jejichž definice zde není přímo uvedena, jsou příslušné definice zejména v čl. 4 Obecného nařízení, odkud níže uvedené také vycházejí.

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.“*

Evidencí se rozumí *„jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.“*

Třetí stranou se rozumí *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který není subjektem údajů, správcem, zpracovatelem ani osobou přímo podléhající správci nebo zpracovateli, jež je oprávněna ke zpracování osobních údajů.“*

Porušením zabezpečení osobních údajů se rozumí *„porušení zabezpečení, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně nebo neoprávněnému poskytnutí nebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných osobních údajů.“*

Dozorovým úřadem se rozumí *„nezávislý orgán veřejné moci zřízený členským státem podle článku 51.“*

4.2 Práva a povinnosti

Správce, zpracovatel a subjekt údajů mají při zpracování osobních údajů určité postavení. Toto postavení také dále vymezuje jejich práva a povinnosti, kterými se buď musí řídit, anebo je mohou uplatňovat. V dalších podkapitolách jsou jednotlivá práva a povinnosti přiblíženy. Specifickou roli zde zastává také pověřenec pro ochranu osobních údajů, který je v dané instituci důležitým kontaktním bodem, a to jak pro její zaměstnance, tak i občany figurující ve vztahu k instituci v roli subjektů údajů, případně také komunikuje s dozorovým úřadem. Zároveň je vhodné uvést, že Obecné nařízení se podle recitálu 27 nevztahuje na osobní údaje zesnulých osob. Členské státy ovšem mohou stanovit pravidla týkající se rovněž zpracování osobních údajů osob zesnulých. V tomto případě ZoZOÚ žádné odlišné podmínky zpracování nestanovuje. Obecné nařízení se rovněž netýká údajů, které získaly a zpracovávají fyzické osoby pro vlastní potřebu, a které jsou pouze osobní povahy (recitál 18), dále anonymizovaných údajů a údajů pro statistické nebo výzkumné účely (recitál 26). Pro představu, po anonymizaci se vytrácí možnost konkrétního přiřazení údajů k dané osobě, kdežto pseudonymizace pouze zakryje určité údaje, které je možné opětovně přiřadit (viz také kap. 4.3.3).

4.2.1 Správce

Správce je faktickým ručitelem, že zpracování osobních údajů probíhá nejen zákonným způsobem, ale také bezpečným způsobem neohrožující subjekt údajů z pohledu vyzrazení, zneužití nebo neoprávněného nakládání s jeho údaji. Obecné povinnosti navázané na správce (v rámci této práce obecně míněno státní instituci) rozvádí čl. 24 až 27 Obecného nařízení. Více jsou jeho povinnosti rozvedeny v mnoha dalších článcích, potažmo recitálech, které konkretizují jednotlivé prvky, jež musí správce naplňovat nebo dodržovat (zásady zpracování, dokumentace, zabezpečení, transparentnost, informovanost subjektů údajů, lhůty pro uchování dat, likvidace, změny atp.). Proto je možné vnímat, že například jednotlivá práva subjektu údajů (viz kap. 4.2.3) jsou do jisté míry povinností správce, aby tato práva plnil, vyjma těch případů, kdy právo správce převažuje nad právem subjektu údajů.

V rámci ZoZOÚ jsou pak upřesněna další oprávnění a výjimky zpracování, kterými český zákonodárce doplňuje výklad Obecného nařízení. Pro státní úřady či instituce jsou podstatná ust. § 1 až § 23 ZoZOÚ, případně ust. § 54 (komunikace s dozorovým úřadem), ust. § 58 (přístup dozorového úřadu k informacím) a ust. § 62 (přestupky). Ustanovení § 24 až § 49 jsou vymezeny pro činnost policejních orgánů[19]. Pokud však bude některá instituce dodržovat povinnosti osob při zabezpečení osobních údajů uvedených v ust. § 46 až § 47 (například povinnost mlčenlivosti), výmaz osobních údajů v ust. § 48, anebo ochranu práv subjektu údajů v ust. § 49, nelze namítat, že by to bylo špatně, jelikož tato ustanovení lze vztáhnout i na běžnou praxi ostatních, v tomto případě státních institucí, byť jsou pragmaticky umístěny v hlavě čtvrté ZoZOÚ pojednávající o ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky. Primární je však stále Obecné nařízení.

a) Odpovědnost správce (čl. 24)

Ve vztahu ke zpracovávaným osobním údajům je správce odpovědný za zavedení patřičných technických a organizačních opatření, které jsou následně uceleným souborem sloužícím jako podklad pro doložení řádného zpracování osobních údajů podle Obecného nařízení, včetně vhodně zvolených koncepcí uplatňovaných správcem na ochranu těchto údajů, které by měly být přiměřené ve vztahu k prováděným činnostem zpracování. Tento článek také pojednává o kodexech chování (čl. 40) a vydávání osvědčení (čl. 42). Dlužno dodat, že ani jeden z těchto konceptů není reálně příliš využíván. Pokud správce chce dodržovat zásady ochrany osobních údajů a plnit povinnosti s tím spojené, může si samozřejmě ověřit, že naplňuje kodex chování uvedený v čl. 40 odst. 2.

b) Záměrná a standardní ochrana osobních údajů (čl. 25)

Při určení prostředků sloužících ke zpracování osobních údajů, tak i v době jejich zpracování, zavede správce vhodná technická a organizační opatření (např. pseudonymizace), jejichž účelem je provádět v instituci zásady ochrany osobních údajů (např. minimalizace), a to účinným způsobem s nezbytnými

[19] Policejní orgán konkretizuje ust. § 12 odst. 2 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

zárukami pro jejich zpracování. Správce přitom přihlédne ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody osob. Zároveň správce zavede taková technická a organizační opatření, aby se zpracovávaly pouze osobní údaje nezbytné pro konkrétně stanovený účel. Tato povinnost se týká množství shromážděných osobních údajů, rozsahu jejich zpracování, doby jejich uložení a jejich dostupnosti (v případě potřeby), což má zajistit, aby osobní údaje nebyly bez pokynu nebo zásahu člověka (předpokládejme odpovědného zaměstnance) zpřístupněny neoprávněné osobě nebo okruhu takových osob.

c) Společní správci (čl. 26)

Tento článek pojednává o společných správcích, kdy účely a prostředky zpracování stanovují dva a více správců společně. Ti poté mezi sebou vymezí své podíly na odpovědnosti za plnění povinností podle Obecného nařízení. Příkladem společných správců mohou být například svazky obcí[20].

d) Zástupci správců nebo zpracovatelů, kteří nejsou usazeni v Unii (čl. 27)

Tento článek se dotýká místní působnosti a týká se správců nebo zpracovatelů, kteří zpracovávají osobní údaje subjektů údajů v prostředí EU, a to správcem nebo zpracovatelem, který není v EU usazený, pokud takové činnosti zpracování souvisí s nabídkou zboží nebo služeb, anebo s monitorováním jejich chování. Tato povinnost se však neuplatňuje na orgán veřejné moci nebo veřejný subjekt. Obecně však správce, a to i státní instituce, musí uvádět, zda při zpracování osobních údajů dochází k jejich předání do třetích zemí nebo mezinárodní organizaci. V souvislosti se systémem pro registraci na poskytnutí státního příspěvku na dítě u Ministerstva práce a sociálních věcí České republiky bylo například následně zjištěno, že data proudí do zahraničí k dalšímu zpracování[21].

---

[20] Když se řekne svazek obcí | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ [cit. 23.08.2022]. Dostupné z: https://www.epravo.cz/top/clanky/kdyz-se-rekne-svazek-obci-108643.html

[21] Formulář na dávky už neposílá adresy do zahraničí, ministerstvo práce ho upravilo | iROZHLAS - spolehlivé zprávy. *iROZHLAS - spolehlivé a rychlé zprávy* [online]. Copyright © 1997 [cit. 22.08.2022]. Dostupné z: https://www.irozhlas.cz/zpravy-domov/mpsv-davky-formular-data-gdpr_2208191910_cib

K uvedení samotné charakteristiky správce lze doplnit, že se jedná o subjekt, který sám, anebo společně s jinými subjekty v roli správce (což není u státních institucí zmiňovaných v této práci příliš obvyklé) určuje účely zpracování a vhodné prostředky, které pro to budou užity, nevyplývá-li to z přímo použitelného právního předpisu. Správci jsou nebo mohou být zároveň také příjemci osobních údajů. **Příjemcem** osobních údajů se podle čl. 4 odst. 9 Obecného nařízení 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*“. Určitou výjimku pak tvoří OVM v případě získání osobních údajů v rámci zvláštního šetření (o skutkovém stavu věci) v souladu s právem členského státu nebo EU, kdy se v takovém případě za příjemce nepovažují.

Správce má za povinnost kromě výše uvedeného dodržovat základní zásady zpracování osobních údajů vyplývající z čl. 5 Obecného nařízení (viz kap. 4.2.4), dále umožnit subjektu údajů výkon jeho práv (viz kap. 4.2.3), jmenovat pověřence pro ochranu osobních údajů (viz kap. 4.2.5) a v případě potřeby komunikovat s dozorovým úřadem (viz kap. 4.6), a to například při hlášení porušení zabezpečení osobních údajů. Může ovšem také osobní údaje zpracovávat bez souhlasu subjektu údajů. Původní ZoOOÚ vymezoval uvedenou možnost v ust. § 5 odst. 2, a také v ust. § 9. Pro změnu ZoZOÚ má toto uvedeno v ust. § 43 odst. 3, ačkoli uvedené je zde upřesněno pro ochranu osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky. Státní instituce se bude řídit Obecným nařízením, které toto uvádí v čl. 6. Pro příklad současného zpracování bez souhlasu lze zmínit např. zpracování pro účely archivnictví, které se řídí zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, anebo zpracování zvláštní kategorie osobních údajů bez souhlasu subjektu údajů z důvodů veřejného zájmu v oblasti veřejného zdraví, jak uvádí recitál 54 Obecného nařízení. Dalším takovým zpracováním může být zpracování pro účely vědeckého nebo historického výzkumu či pro statistické účely.

Pokud se přesuneme k více praktické části, každý správce musí mít stanoven vnitropodnikový předpis upravující ochranu osobních údajů (viz kap. 4.3.1). Tento dokument ve formě interní směrnice nebo příkazu (eventuálně závazného pokynu) má stanovit základní postupy (včetně dokumentace), kterými se bude instituce řídit a zaměstnanci je budou dodržovat. Povinností správce by mělo být tento interní dokument vydat, a dále pravidelně aktualizovat o další změny v rámci příslušné legislativy, ať již unijní, tak vnitrostátní, popřípadě také u změn příloh k tomuto dokumentu. Za správce se pak považuje nejvyšší vedení instituce, které může (a často tak také činí) tyto pravomoci přenést na nižší linie vedení, potažmo další k tomu pověřené zaměstnance. Obecně řečeno je tedy správcem instituce, oficiálně pověřeným vykonavatelem za správce (tedy osoba pověřená plněním povinností správce) pak budou ředitelé jednotlivých úseků, kteří toto budou s největší pravděpodobností přenášet na jim podřízené vedoucí zaměstnance (ředitelé či vedoucí odborů a oddělení), kteří je budou o plnění povinností informovat.

Správce v dané roli pak bude mít zejména tyto povinnosti:

a) stanovit účel, prostředky a způsob zpracování osobních údajů
b) vést záznamy o činnostech zpracování a v případě potřeby je aktualizovat
c) zajistit soulad zpracování osobních údajů s Obecným nařízením a se ZoZOÚ, a být schopen tento soulad doložit
d) podle potřeby uzavřít písemnou smlouvu se zpracovatelem osobních údajů o jejich zpracování (viz kap. 4.2.2),
e) na vyžádání spolupracovat s dozorovým úřadem při plnění jeho úkolů a být schopen mu předložit aktuální dokumentaci
f) implementovat vhodná technická a organizační opatření za účelem zajištění a prevence bezpečnosti zpracovávaných osobních údajů, a v případě potřeby je aktualizovat (může být podloženo dalšími dokumenty), viz kap. 4.3.3
g) zohledňovat rizika pojící se s ochranou osobních údajů (například ztráta, zničení, pozměnění nebo neoprávněné zpřístupnění), viz také kap. 4.3.4
h) zajistit výkon práv subjektu údajů (viz kap. 4.2.3), pro což je vhodné mít zajištěn interní postup (může být přímo ve směrnici nebo přílohou k ní)

i) ohlašovat dozorovému úřadu porušení zabezpečení osobních údajů, pakliže k takové okolnosti dojde, a to bez zbytečného odkladu (nejlépe do 72 hodin), a je povinen toto dokumentovat (viz kap. 4.2.8), mimo výjimek
j) oznámit subjektu údajů porušení zabezpečení, které bude mít vysoké riziko pro jeho práva a svobody, mimo výjimek (viz kap. 4.2.3 písm. l))
k) dokázat plnit informační povinnost vůči subjektu údajů (viz kap. 4.2.3 písm. b) a c))
l) v případě potřeby být schopen provádět posouzení vlivu na ochranu osobních údajů, případně také balanční test (viz kap. 4.3.5)
m) provádět pravidelnou kontrolu zabezpečení ochrany osobních údajů (může být odpovědností vedoucích zaměstnanců na pracovišti jejich podřízených, případně formou metodické dohlídky od oprávněných zaměstnanců)
n) další povinnosti, které mu jsou uloženy interním dokumentem (například doložit plnění povinností vyplývajících z interního dokumentu a předat příslušné podklady, které toto dokládají na určené oddělení či určené osobě)

Povinnosti správců také rozvádí na svých webových stránkách dozorový úřad, kde lze v příslušných rubrikách najít další cenné informace[22]. Pro shrnutí jsou při naplňování Obecného nařízení a ZoZOÚ klíčovými povinnostmi zejména komunikace se subjekty údajů a plnění informační povinnosti, jmenování pověřence a komunikace s ním ve věcech zabezpečení a oprávněnosti zpracování osobních údajů, zajišťování bezpečnostních pravidel a povinností při zpracování, nakládání a jiné manipulaci s osobními údaji, vedení příslušné dokumentace a provádění její aktualizace, zvažování rizik spojených se zpracováním osobních údajů a nastavování tomu odpovídajících opatření, včetně komunikace s dozorovým úřadem u bezpečnostních incidentů (kromě výjimek) nebo na dožádání úřadu při prováděné kontrole. Uvedené ovšem nepůjde konat zcela hladce, pokud nebudou pro tyto úkony určeni zaměstnanci, jejichž odpovědností bude zajistit aplikaci těchto prvků v prostředí instituce, včetně umožnění komunikace s pověřenými, a také kvalifikovanými osobami.

[22] Povinnosti správců: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 26.08.2022]. Dostupné z: https://www.uoou.cz/povinnosti-spravcu/ds-5856/p1=5856

4.2.2 Zpracovatel

Zpracovatelem je v podstatě subjekt, na který správce přenáší povinnost úplného nebo částečného zpracování osobních údajů, nikoli však odpovědnost, která je stále vztažena na správce. Ten si proto musí nechat od zpracovatele doložit takové záruky, kterými zpracovatel potvrdí, že zpracování osobních údajů na jeho straně je srovnatelné s implementovanými prvky ochrany osobních údajů u správce (technická a organizační opatření), a tedy že má nastavena taková pravidla zabezpečení zpracování, která jsou na stejné nebo vyšší úrovni, aby byla zajištěna ochrana práv subjektu údajů. Zároveň by tyto podmínky plnění měly být uvedeny ve smlouvě, kterou správce se zpracovatelem uzavírá. Typickým příkladem smlouvy se zpracovatelem u státní instituce může být například smlouva s bezpečnostní agenturou, která bude zajišťovat dohled a bezpečnost při vstupu do budovy, včetně přidružených činností s tím spojených. Správce může od zpracovatele požadovat také předložení bezpečnostních záruk nebo certifikátů o naplnění určité bezpečnostní úrovně, popřípadě auditní výstupy reflektující tento fakt. Sám je pak oprávněn v rámci prověřování naplnění opatření provést dohlídky přímo u zpracovatele, což se považuje za rozhodně vhodné, aby se případně předešlo nesrovnalostem, anebo napravil možný závadný stav. Porušení bodů smlouvy bývá sice podmíněno sankcemi, ale prevence je často lepší varianta než náprava způsobených škod.

V původním ZoOOÚ bylo v ust. § 10 uvedeno, že zpracovatel rovněž dbá při zpracování osobních údajů na to, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů. Zároveň se v ZoOOÚ uvádí v ust. § 7, že povinnosti vztahující se na správce uvedené v § 5 platí také pro zpracovatele. Ani v tomto případě není odchýlení se nijak zásadní. V novém ZoZOÚ se často prolíná plnění povinností správce a zpracovatele. Samotný zpracovatel je pak ukotven v ust. § 34. Jak již bylo ovšem zmíněno, ustanovení uvedená v § 24 až § 49 se vztahují na policejní orgány, a proto je potřeba se řídit u zpracovatele čl. 28 a 29 v Obecném nařízení, popřípadě recitály v Obecném nařízení, například recitál 81. V dalších recitálech jsou často uváděny obecné povinnosti pro správce a zpracovatele.

Informační povinnost o zpracovatelích správce podává buď obecně nebo konkrétně, v závislosti na smluvním zajištění zpracovatele a na předmětu plnění jeho činnosti pro správce. Zpracovatel by neměl do zpracování zapojovat ani žádného dalšího zpracovatele bez předchozího nebo písemného svolení od správce (čl. 28 odst. 2 Obecného nařízení). Zpracování samotné se řídí právně závaznou smlouvou, která musí být vyhotovena jak písemně, tak elektronicky (čl. 28 odst. 9 Obecného nařízení). Zpracovatel se v ní zavazuje správci k plnění různých podmínek. Je vhodné proto zajistit, aby taková smlouva byla řádně připravena, prokonzultována mezi právním a bezpečnostním oddělením, stejně tak i s pověřencem pro ochranu osobních údajů. Nevyplývá-li pro zpracovatele zpracování osobních údajů z právního předpisu, musí být mezi správcem a zpracovatelem uzavřena smlouva o zpracování.

Smlouva se zpracovatelem pak obecně obsahuje nebo stanovuje podle čl. 28 odst. 3 Obecného nařízení tyto činnosti a informace: „předmět a dobu trvání zpracování; povahu a účel zpracování; typ osobních údajů a kategorie subjektů údajů; povinnosti a práva správce“. Dále pak podle tohoto článku zpracovatel přistupuje k níže uvedenému:

a) Zpracovává osobní údaje pouze na základě doložených pokynů správce (včetně předání do třetí země nebo mezinárodní organizaci)
b) Zajišťuje zákonnou povinnost mlčenlivosti u osob oprávněných zpracovávat osobní údaje, popřípadě k ní oprávněné osoby zavazuje
c) Přijme opatření podle čl. 32 Obecného nařízení, čímž se rozumí provedení vhodných technických a organizačních opatření při zabezpečení zpracování
d) Dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odst. 2 a 4 čl. 28 Obecného nařízení (upřesňuje tamtéž například recitál 109)
e) Zohledňuje povahu zpracování, je správci nápomocen prostřednictvím technických a organizačních opatření a reaguje za správce (je-li to možné) na žádosti o výkon práv subjektu údajů
f) Pomáhá v případě potřeby správci při zajištění souladu s čl. 32 až 36 Obecného nařízení při zohledňování povahy zpracování

g) Na pokyn správce vymaže nebo vrátí veškeré os. údaje správci po ukončení poskytování služeb (včetně kopií)
h) Poskytne správci veškeré informace potřebné k doložení skutečnosti o plnění těchto povinností a umožní správci provést audit ke kontrole naplňování zavedených opatření

Často bývá také zvykem, že podmínky zpracování osobních údajů mohou být v dané smlouvě zakomponovány v rámci jednoho bodu, kde budou podrobněji rozvedeny, a nemusí se tedy jednat o smlouvu vyloženě pouze pro tyto účely. Co je ovšem důležité a nemělo by se to brát na lehkou váhu, je odpovědné stanovení jednotlivých podmínek komplexně za celou smlouvu. Nemělo by tedy docházet k situacím, kdy se pouze přejímá obecná předpřipravená forma, která nebude zohledňovat smluvní skutečnosti a požadavky. Také není vhodné do smlouvy například uvést jeden odstavec, že zpracovatel je vázán Obecným zařízením a plní podmínky z něj vycházející. Podmínky musí být stanoveny konkrétně, jasně a transparentně pro obě strany, a při jejich stanovení je nutné přečtení celého dokumentu a vyhodnocovat každou připravovaný smluvní akt samostatně, byť se samozřejmě dá předpokládat, že některá ustanovení se budou podobat nebo opakovat.

Zpracovatel jedná vždy na pokyn správce a na základě jeho pokynů osobní údaje zpracovává vyjma případů, kdy by jim tuto povinnost ukládalo právo členského státu nebo EU. V případě porušení smluvních povinností má zpracovatel kromě sankcí stanovených ve smlouvě také odpovědnost podle čl. 82 Obecného nařízení, navazující dále čl. 83 a čl. 84. Závěrem lze ještě doplnit, že k tomu určený subjekt je *„zpracovatelem pouze ve vztahu k osobním údajům poskytnutým správcem, nikoli osobních údajů, které zpracovává pro účely, které se jej přímo dotýkají (například je správcem při zpracování osobních údajů vlastních zaměstnanců)“*[23]. Při komparaci s původním ZoOOÚ je definice zpracovatele co do smyslu obdobná jako v Obecném nařízení.

[23] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi, s. 32.

4.2.3 Subjekt údajů

Subjekt údajů je v oblasti ochrany osobních údajů zřejmě tím nejdůležitějším prvkem (v kontextu celého smyslu Obecného nařízení). Je to právě subjekt údajů, jehož osobní údaje (případně také osobně identifikovatelné informace[24]) a práva jsou hájeny. Je jim také přikládán velký význam, kdy při neoprávněném nakládání či zpracování takových údajů, anebo při porušování práv dochází k udělování pokut (leckdy velmi vysokých), v lepším případě k uložení nápravných opatření (resp. opatření k nápravě). Subjekt údajů má primárně ukotvena svá práva v čl. 12 až 22 Obecného nařízení, která se týkají práva na transparentní a srozumitelné podávání informací o zpracování, práva na poskytnutí informací od správce o údajích získaných nebo nezískaných od subjektu údajů, práva na přístup, opravu, výmaz, omezení, přenositelnost, dále práva vznést námitku a automatizovaného rozhodování. Trochu stranou pak stojí právo odvolat souhlas uvedené v čl. 7 odst. 3, a v čl. 34 povinnost správce oznámit subjektu údajů porušení zabezpečení. Podrobněji jsou tato oprávnění rozvedena v následujících bodech označených písmeny a) až l).

a) Transparentnost (čl. 12)

První z řady práv (v tomto případně lze hovořit také o zásadě) paralelně říká, na co má subjekt údajů právo, a zároveň co by měl správce naplnit. Nejedná se o právo nové, nýbrž vycházející již z předchozí právní úpravy nebo judikatury soudů. Spočívá v právu na informace o zpracování osobních údajů, které mají být sděleny transparentně, tj. ve stručné, jasné, jazykově srozumitelné a jednoduché podobě, a zároveň snadno přístupným způsobem. Sdělení se týká veškerých informací uvedených v čl. 13 a v čl. 14, včetně sdělení podle čl. 15 až 22, případně čl. 34. Informace mají být poskytnuty vhodnými prostředky buď v písemné nebo elektronické podobě. Na žádost subjektu údajů mohou být tyto informace poskytnuty také ústně. Správce rovněž poskytne informace o přijatých opatřeních, které učinil (podle čl. 15 až 22) ve lhůtě do jednoho měsíce (lhůta může být v odůvodněných případech prodloužena, maximálně však o dva měsíce). Podstatou transparentního sdělení je, aby subjekt údajů po přečtení

[24] Vychází z normy ISO/IEC 27018 o veřejných cloudových službách a ochraně osobních dat

informací neměl problém porozumět psanému textu, aby mu bylo zřejmé, jak a pro jaký účel jsou jeho osobní údaje zpracovávány, mají mu být sdělena jeho práva, pokud s takovým zpracováním nesouhlasí, a zároveň by se měl k těmto informacím dostat snadnou cestou, například na webových stránkách instituce, kde bude uveden odkaz, pod kterým se subjekt údajů veškeré podstatné informace dozví. Nemělo by se tedy například stát, že v informacích uváděných správcem budou nesrozumitelné výrazy, příliš cizích nebo neznámých slov nebo složité formulace. U informací podávaných dítěti se upřednostňuje jednoduchost a případně využití vizualizace (recitál 58). Co se týče sdělení informací na webových stránkách, měl by mít subjekt údajů k těmto informacím snadnou cestu a neměl by se proklikávat přes různá témata a odkazy. Při každém novém zpracování musí být tyto informace aktualizovány. Subjekt údajů může být informován také písemnou cestou, i zde platí co do obsahu a lhůt stejné podmínky. Důležité je, aby správce na žádost subjektu údajů vždy reagoval.

b) Informace získané od subjektu údajů (čl. 13)

V případě, že osobní údaje poskytuje přímo subjekt údajů, podává správce informace v okamžiku jejich poskytnutí (resp. získání od subjektu údajů). Rozsah podávaných informací je: „totožnost a kontaktní údaje správce, případně pověřence, je-li ustanoven (viz kap. 4.2.5); účely zpracování a právní základ (titul) pro zpracování; oprávněné zájmy správce nebo třetí strany (v případě čl. 6 odst. 1 písm. f)); případné příjemce nebo kategorie příjemců osobních údajů; případný úmysl správce předat osobní údaje třetí straně nebo mezinárodní organizaci; doba uložení (případně kritéria pro určení této doby, nebylo-li ji možné určit); poučení o právech subjektu údajů (viz čl. 13 odst. 2 písm. b) až d)); informace, zda poskytování údajů je dáno zákonným či smluvním požadavkem a případné povinnosti či důsledky s tím související; informace o automatizovaném zpracování (příp. profilování), pokud probíhá“. V případě zpracování pro jiný účel, než jaký byl stanoven pro shromáždění údajů, musí správce subjektu údajů poskytnout informace o tomto zpracování. Správce nemusí poskytovat informace podle tohoto článku v případě, že subjekt údajů již má tyto informace v odpovídající míře k dispozici. Předchozí ZoOOÚ upravoval informační povinnost obdobně v ust. § 11 a také v ust. § 21.

c) Informace nezískané od subjektu údajů (čl. 14)

Zde se oproti předchozímu článku pouze rozšiřují povinnosti na zdroj, ze kterého osobní údaje pocházejí, eventuálně se podávají také informace o tom, zda pocházejí z veřejně dostupných zdrojů. Takovouto informaci je potřeba podat v přiměřené lhůtě po získání osobních údajů (nejpozději do jednoho měsíce, avšak také v závislosti na okolnostech jejich zpracování). Informační povinnost není nutné plnit, pokud subjekt údajů (zde jako v předchozím případě) má informace k dispozici, dále pokud by jejich poskytnutí vyžadovalo nepřiměřené úsilí, popřípadě není možné tyto informace poskytnout (například u zpracování pro účely archivace ve veřejném zájmu, anebo pro vědecké či statistické účely), nebo pokud získávání či zpřístupnění údajů je výslovně stanoveno právem, anebo pokud tyto údaje musí zůstat důvěrné na základě právních povinností (služební tajemství a povinnost mlčenlivosti).

d) Právo na přístup (čl. 15)

Subjekt údajů má v tomto případě právo získat od správce informace ve formě potvrzení, jaké osobní údaje jsou o něm správcem zpracovávány a v jakém rozsahu. Po získání potvrzení může obdržet kopii zpracovávaných údajů (za další může správce požadovat přiměřený poplatek). Pokud správce zpracování potvrdí, má subjekt údajů právo na přístup k těmto informacím, mezi něž patří účely zpracování (tzn. jaký má správce důvod k tomu, že tyto informace u sebe udržuje a aktivně či pasivně s nimi nakládá), kategorie osobních údajů (tedy jaké osobní údaje jsou zpracovávány), příjemci údajů včetně třetích zemí a mezinárodních organizací (tzn. komu byly nebo budou osobní údaje zpřístupněny, resp. kdo je jejich příjemcem), doba uložení (tedy jaká je lhůta pro uložení údajů, její odůvodnění, a není-li možné ji zcela vymezit, pak uvést stanovující kritéria určující tuto dobu), místo uložení (tzn. místní určení, kde jsou nebo budou osobní údaje zpracovávány), informace o možnosti učinit podání u dozorového úřadu (tzn. uvést kontaktní informace na dozorový úřad pro případné stížnosti nebo jiné dotazy), zdroj získání údajů (tedy původce informací, nebyl-li jím sám subjekt údajů), a pokud státní instituce toto provádí, pak také uvést veškeré skutečnosti týkající se automatizovaného rozhodování, včetně profilování (ve státních institucích a úřadech státní správy však není

profilování příliš obvyklé, pokud by se objevilo, je nutné uvést informace o postupu takového zpracování, jeho významu a důsledků pro subjekt údajů).

Závěrem tohoto bodu je ještě vhodné zmínit, že se jedná o právo působící erga omnes (tj. vůči všem). Má ovšem své hranice, které stanovuje čl. 23 Obecného nařízení, jež se vztahuje na omezení plynoucí z právního řádu členské země nebo práva EU, kdy subjektu údajů mohou být určitá práva omezena, zároveň však nesmí dojít k ohrožení nebo porušení jeho základních práv a svobod. Příkladem může být předání informací policejnímu orgánu nebo neposkytování informací o jiných subjektech údajů (hájí se práva dalších osob). Při poskytování informací podle zákona o svobodném přístupu k informacím je gestorem pro výklad tohoto zákona Ministerstvo vnitra České republiky.

e) Právo na opravu (čl. 16)

Právo na opravu je charakteristické tím, že správce by měl bez zbytečného odkladu opravit nebo doplnit údaje subjektu údajů, aby odpovídaly skutečnosti. Může se jednak jak o objektivně (nepřesný, ale jinak reálný osobní údaj), tak i subjektivně nepřesné údaje (může se týkat osobního hodnocení od vedoucího zaměstnance, se kterým nemusí být subjekt údajů ztotožněn), a do rozhodnutí o jejich opravě by měl správce jejich zpracování omezit, a informovat o tomto omezení rovněž příjemce údajů. Subjekt údajů má tedy s přihlédnutím k účelům zpracování právo na doplnění těch údajů o jeho osobě, které se mu jeví jako nepřesné nebo nesprávné. Zároveň je to také jeho povinnost, a pokud změnu údajů nenahlásí, nemůže být správce vinen z případných důsledků. V opačném případě, kdy správce údaje na žádost subjektu údajů neopraví, jdou obrazně řečeno veškeré možné důsledky z toho plynoucí za ním. Příkladem z reálného života budiž situace, kdy subjekt údajů nahlásil změnu místa bydliště správci (bankovní instituci), který toto ovšem nereflektoval. S ohledem na probíhající rozvodové řízení subjektu údajů obdržela protistrana výpis z účtu s výší došlé mzdy, včetně odměn a informací o zůstatku na účtu, což subjektu údajů v probíhajícím soudním rozvodovém řízení značně přitížilo. Přestože se jedná o poměrně starší záležitost z dob ještě před příchodem Obecného nařízení, je potřeba se obdobným excesům vyvarovat. Subjekt údajů se ve svém

rozpoložení neodhodlal podat stížnost k dozorovému orgánu ani k soudu, což mohlo správce stát například poškození dobrého jména nebo i zaplacení pokuty. V dnešní době by takový případ mohl mít podstatně horší dopad, obzvláště pokud by se ukázalo, že je těchto případů u správce více.

f) Právo na výmaz (čl. 17)

Právo na výmaz, jinak zmiňované také jako právo být zapomenut, spočívá v právu subjektu údajů požadovat po správci, aby jeho osobní údaje byly bez zbytečného odkladu zlikvidovány. To by měl správce zajistit vnitropodnikovým procesem likvidace. Vždy je však potřeba při obdržené žádosti překontrolovat, zda stále trvá účel a právní titul zpracování. Mezi důvody, které mohou vést k tomuto kroku, patří: „údaje již nejsou potřebné pro účely zpracování; byl odvolán souhlas se zpracováním; subjekt údajů vznesl oprávněnou námitku; údaje byly zpracovávány protiprávně; výmaz stanoví právní předpis; údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti dětem“. Správce následně přijme přiměřené kroky k nápravě stavu. Toto právo nemusí být uplatněno, pokud je zpracování nezbytné pro: „výkon práva na svobodu projevu a informace; splnění právní povinnosti; důvody veřejného zájmu v oblasti veřejného zdraví; účely archivace ve veřejném zájmu nebo účely vědecké, historické či statistické; určení, výkon nebo obhajobu právních nároků (realizace právních nároků)“. Toto právo bylo vyloženo v rozsudku Soudního dvora Evropské unie (ESDS) ve věci Google Spain versus Mario Costeja González[25].

g) Právo na omezení (čl.18)

Subjekt údajů může žádat správce, aby v některých případech omezil zpracování jeho osobních údajů. Dříve se toto právo označovalo jako „právo na blokaci“ a v ZoOOÚ bylo označováno termínem blokování. Pokud dojde k omezení zpracování, nezpracovává správce údaje subjektu údajů jinak než jejich uložením. Důvodem pro omezení je: „subjekt údajů popírá přesnost údajů;

[25] Bulletin advokacie, odborný právnický portál | Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie, odborný právnický portál | Domů* [online]. Copyright © [cit. 17.08.2022]. Dostupné z: http://www.bulletin-advokacie.cz/analyza-praktickych-dopadu-rozhodnuti-soudniho-dvora-eu-ve-veci-google-spain

zpracování je protiprávní, ale subjekt údajů odmítá výmaz; u správce pominuly účely zpracování, avšak subjekt údajů potřebuje tyto údaje k realizaci právních nároků; subjekt údajů vznesl námitku podle čl. 21“. V jakémkoli jiném případě musí být pro zpracování dán souhlas subjektu údajů nebo je důvodem pro zpracování např. realizace právních nároků, ochrana práv jiné fyzické nebo právnické osoby či důležitý veřejný zájem.

h) Právo na přenositelnost (čl. 20)

Jak může napovědět samotný název, jedná se o právo, které má usnadnit přechod mezi poskytovateli služeb, a také usnadnit přesun patřičných dat, resp. osobních údajů. Pro subjekt údajů to znamená, že má oprávnění získat od správce své osobní údaje, které mu poskytl, a předat je jinému správci, aniž by tomu předchozí správce různými obstrukcemi bránil. Uvedené lze uskutečnit v případech, kdy je zpracování založeno na souhlasu nebo smlouvě, anebo pokud je zpracování prováděno automatizovaně. Vykonání tohoto práva nemusí nutně znamenat ukončení zpracování u původního správce. Není tak dotčen čl. 17, a zároveň se toto právo neuplatní u zpracování prováděném ve veřejném zájmu nebo při výkonu veřejné moci, jímž je správce pověřen. Subjekt údajů má také při uplatňování tohoto práva nárok, aby jeho osobní údaje byly předány jedním správcem přímo jinému správci (za předpokladu technické proveditelnosti). Obecně řečeno, k přenosu dat se přistoupí, pokud se jedná o aktivně poskytnuté údaje, anebo údaje vysledované za pomoci využívání některých služeb. Neměly by se ovšem poskytovat údaje odvozené od údajů poskytnutých subjektem údajů. Při přímém poskytování dat od subjektu údajů by měl správce dbát příslušného zabezpečení při přenosu, aby nedošlo k úniku dat vlivem neopatrného, neodborného nebo závadného jednání.

i) Právo vznést námitku (čl. 21)

V tomto případě se jedná o obdobu práva na odvolání souhlasu. Subjekt údajů má právo vznést námitku proti zpracování jeho osobních údajů, čímž jinak řečeno požaduje ukončení zpracování těchto údajů pro konkrétní účely. Správce je povinen žádosti vyhovět, pokud pro takové zpracování neprokáže závažné oprávněné důvody, které by převažovaly nad právy a svobodami subjektu údajů,

případně důvody k realizaci právních nároků. Právo vznést námitku se tedy uplatní u takového zpracování, které je založeno na plnění úkolu správce prováděném ve veřejném zájmu nebo při výkonu veřejné moci (čl. 6 odst. 1 písm. e)), anebo na oprávněném zájmu správce (čl. 6 odst. 1 písm. f)). Pokud by se jednalo o přímý marketing, námitku je možné vznést kdykoli, a takové žádosti musí být vždy vyhověno.

j) Automatizované rozhodování a profilování (čl. 22)

V tomto článku se fakticky setkáváme se dvěma pojmy, a to s automatizovaným individuálním rozhodováním a profilováním. Obojí se často prolíná nebo doplňuje, ale uvedené je možné provádět také separovaně a tyto činnosti nemusí být vzájemně propojené. Právo nebýt předmětem automatizovaného zpracování bylo již součástí Směrnice 95/46/ES, včetně ZoOOÚ (§11 odst. 6), a je zásadní proto, aby nedocházelo k výhradně automatizovanému rozhodování s právními nebo obdobnými účinky vůči subjektu údajů[26]. Automatizovaným rozhodováním můžeme rozumět použití technických prostředků při zpracování osobních údajů, přičemž se jedná zejména o samořídící algoritmy, které pracují nezávisle na lidském vstupu, který je uvažován pouze na začátku při zadání vstupních požadavků (resp. hodnot) do systému, přičemž další procesy by probíhaly automaticky. Příkladem takového zpracování, které není v praxi možné, by bylo automatické zasílání rozhodnutí o přestupku na základě uvedeného automatizovaného rozhodování, ačkoli by co do technických možností bylo již snadno uskutečnitelné[27]. Možné je pouze v případě, je-li nezbytné k uzavření nebo plnění smlouvy mezi správcem a subjektem údajů, dále je-li povoleno právními předpisy členského státu či právem EU, anebo je-li takové zpracování založeno na výslovném souhlasu subjektu údajů. Subjekt údajů by měl mít právo vědět a být zároveň informován, v čem spočívá logika automatizovaného zpracování osobních údajů, jaké mohou být důsledky takového zpracování (zejména v případě návaznosti na profilování) a kdo jsou příjemci zpracování (recitál 63). Další doplnění pak podává ust. § 36 ZoZOÚ.

[26] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 148.
[27] Tamtéž, s. 148.

Recitál 68 ještě uvádí, že pokud se osobní údaje zpracovávají automatizovaně, měl by subjekt údajů mít též právo získat osobní údaje, které se ho týkají, a jež poskytl správci, ve strukturovaném, běžně používaném, strojově čitelném a interoperabilním formátu (např. pro předání jinému správci).

Zvláštní kategorie osobních údajů pak mohou být pro automatizované rozhodování využity pouze v případě, že subjekt údajů dal výslovný souhlas (čl. 9 odst. 2 písm. a) Obecného nařízení), nebo pokud je zpracování nezbytné z důvodu významného veřejného zájmu (čl. 9 odst. 2 písm. g) Obecného nařízení) a zároveň jsou zavedena vhodná opatření pro práva a svobody a oprávněných zájmů subjektu údajů[28]. Pokud se nejedná ani o jeden z těchto případů, má subjekt údajů právo nebýt předmětem žádného rozhodnutí založeném na automatizovaném zpracování, včetně profilování.

Profilování pak lze označit za další formu automatizovaného zpracování, které spočívá v trvalém získávání osobních údajů, jejich monitorování a vyhodnocování na základě chování subjektu údajů. Ve státních institucí se profilování ve většině případů nevyužívá. Profilování je typické pro ekonomické zájmy obchodních korporací. Více informací poskytuje dále například recitál 24 nebo 30. Také zde by pak platilo, že subjekt údajů by měl být dále informován o profilování a o jeho důsledcích. Dále pak téma rozvádí např. recitál 70 nebo 71, který přímo definuje tento pojem. Téma vysvětlují i různé elektronické zdroje[29].

k) Odvolání souhlasu (čl. 7)

Právo na odvolání souhlasu je součástí řady práv, které má subjekt údajů v rámci Obecného nařízení k dispozici. Před jeho příchodem byl souhlas považován za tradiční faktor, který umožňoval zpracování osobních údajů. S příchodem Obecného nařízení došlo k určité a vítané změně, jelikož souhlas

[28] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 149.

[29] Profilování a automatizované rozhodování | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. [cit. 17.08.2022]. Dostupné z: https://www.gdpr.cz/blog/profilovani/

subjektu údajů byl upozaděn před jinými zákonnými podmínkami pro zpracování. Nyní k němu má být přistupováno pouze tehdy, pokud není jiná alternativa vycházející z čl. 6 odst. 1 Obecného nařízení. Čl. 7 stanovuje podmínky vyjádření, včetně možnosti odvolání. Odvoláním souhlasu zároveň nesmí být dotčena zákonnost zpracování vycházející ze souhlasu, který byl dán před jeho odvoláním. Pro příklad z praxe lze uvést registraci subjektu údajů do státního systému elektronických aukcí. V případě, že se subjekt údajů pouze registruje, ale nevstoupí do žádné aukce svou nabídkou, může svůj souhlas se zpracováním osobních údajů odvolat a požadovat kompletní odstranění svých údajů ze systému. V opačném případě, kdy se aktivně účastnil nejméně jedné z prováděných aukcí, je sice možné souhlas odvolat, ale nedojde k výmazu poskytnutých údajů, jelikož zde převažuje právní zájem pro doložení zákonných podmínek, za nich se předmětná aukce mohla uskutečnit.

l) Oznámení o porušení zabezpečení (čl. 34)

Jedná se zde o povinnost správce, ale zároveň také o právo subjektu údajů být informován o jakémkoli porušení zabezpečení, které může mít pro subjekt údajů vysoké riziko pro jeho práva a svobody. V dnešní době existují rizika, která správce nemusí reflektovat a subjekt údajů o nich pravděpodobně ani nebude vědět. Pokud dojde k tomu, že se riziko přemění ve skutečnost, může vést k fyzické, hmotné nebo nehmotné újmě pro subjekt údajů (více recitál 75). V takovém případě by měl správce bez prodlení oznámit subjektu údajů, že toto porušení může mít za následek vysoké riziko pro jeho práva a svobody, aby mohl učinit nezbytná opatření. V oznámení uvede povahu porušení zabezpečení včetně informace a opatření plynoucí z čl. 33 odst. 3 písm. b), c) a d). Od oznámení lze za určitých podmínek upustit, např. pokud správce zavedl náležitá technická a organizační opatření k nápravě stavu (viz také kap. 4.2.8).

Při krátkém pohledu na původní ZoOOÚ je možné ještě doplnit, že u zpracování osobních údajů měl správce dbát podle ust. § 10 ZoOOÚ na to, „*aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů*“. Další povinnosti se uvádí

například v ust. § 11 odst. 1 ZoOOÚ, kdy „*Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21*“ (Ochrana práv subjektů údajů). Takovýchto plnění je ve zmíněném předpise uvedeno více. Původní ZoOOÚ byl do značné míry uceleným právním předpisem, který poskytoval dostatečné záruky a opatření, která bohužel v praxi nebyla příliš naplňována, ale samotný předpis již aplikoval mnohá opatření ze Směrnice 95/46/ES.

4.2.4 Základní zásady zpracování

Základní zásady zpracování jsou významným prvkem v celém procesu ochrany osobních údajů. Správce i zpracovatel mají povinnost podle těchto zásad postupovat a naplňovat je. Jedna ze zásad již byla zmíněna v kapitole 4.2.3, a to zásada transparentnosti. Zásady zpracování představuje a rozvádí čl. 5 Obecného nařízení, anebo také čl. 47 odst. 2 písm. d) tohoto nařízení. Pro další informace lze nahlédnout například na stránky dozorového úřadu[30] nebo Ministerstva vnitra České republiky[31]. Níže jsou jednotlivé zásady rozvedeny.

a) Zásada zákonnosti, korektnosti a transparentnosti

Zpracování musí být zákonné, což více upřesňuje čl. 6 Obecného nařízení. Mezi zákonné podmínky zpracování řadíme: “udělení souhlasu subjektu údajů; zpracování je nezbytné pro plnění smluvního vztahu, ve kterém je subjekt údajů smluvní stranou; zpracování je nezbytné pro splnění právní povinnosti vztahující se na správce; zpracování je nezbytné pro ochranu životně důležitých zájmů

[30] 4. Zásady a právní důvody zpracování: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 29.08.2022]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271

[31] Zásady zpracování osobních údajů - Ochrana osobních údajů. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2022 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 29.08.2022]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx

subjektu údajů; zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci kterým je správce pověřen; zpracování je nezbytné pro účely oprávněných zájmů správce“. Souhlas se nepoužije v případě, pokud se aplikuje čl. 6 odst. 1 písm. b), c) nebo e) Obecného nařízení. V případě čl. 6 odst. 1 písm. d) musí být souhlas udělen bez zbytečného odkladu, jakmile to okolnosti dovolí (zpracování nezbytné pro ochranu životně důležitých zájmů subjektu údajů). Pokud se bude uplatňovat pro zpracování čl. 6 odst. 1 písm. f) měl by být souhlas udělen, anebo učiněno jiné seznámení subjektu údajů se zpracováním jeho osobních údajů (zpracování nezbytné pro účely oprávněných zájmů správce), což se netýká zpracování prováděného OVM při plnění jejich úkolů. V rámci uvedeného písm. f) hovoříme například o kamerovém systému (viz kap. 4.5), jehož účelem je ochrana majetku správce, anebo o vstupních identifikačních kartičkách zaměstnanců.

Samotný souhlas se zpracováním osobních údajů nesmí být upřednostňován před jinými druhy zpracování, což znamená, že nesmí být právním důvodem pro zpracování osobních údajů v takových případech, kdy je možné zpracování na základě jiného právního titulu. Tím může být například plnění smluvního vztahu se subjektem údajů, plnění právní povinnosti správce nebo realizace jeho práv a povinností, či plnění úkolů prováděné ve veřejném zájmu. V takových případech se souhlas neuplatní a ani nesmí být vyžadován. Podmínky vyjádření souhlasu stanovuje čl. 7 Obecného nařízení.

Transparentnost následně rozvádí čl. 12, který vymezuje, že správce musí přijmout vhodná opatření, aby byl schopen subjektu údajů poskytnout stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jazykově srozumitelných vyjádření veškeré informace uvedené v čl. 13 a v čl. 14 Obecného nařízení, a další sdělení podle čl. 15 až 22 tamtéž (viz kap. 4.2.3).

Korektnost má zajistit, že poskytnuté informace budou odpovídat skutečnému stavu věci a bude zachována odpovídající komunikace mezi správcem a subjektem údajů, stejně tak i dodržování ustanovení vyplývajících z nařízení.

b) Zásada účelovosti

Neméně důležitá je zásada vypovídající o účelu zpracování. Shromažďování osobních údajů musí být pro určité, výslovně vyjádřené a legitimní účely, kdy osobní údaje nesmějí být zpracovávány způsobem, který by byl s těmito stanovenými účely v rozporu (výjimkou jsou například účely archivace ve veřejném zájmu nebo účely vědeckého a historického výzkumu či statistické účely)

c) Zásada přiměřenosti

Neboli také zásada minimalizace údajů, kdy jsou osobní údaje zpracovávány pouze v nezbytně nutné míře a ve vztahu k předmětnému účelu plnění. Pokud tedy bude pro nějaký úkon postačovat, aby subjekt údajů uvedl své jméno, datum narození a místo bydliště, neměl by správce požadovat a zpracovávat jakékoli další údaje.

d) Zásada přesnosti

Také jako zásada správnosti údajů, vypovídá o tom, že údaje musí být přesné, na žádosti subjektu údajů bezodkladně aktualizované, nebrání-li tomu výkon jiné povinnosti nebo ověření faktických skutečností, kdy může být zpracování pozastaveno do doby ověření.

e) Zásada omezení uložení

Při této zásadě dbá správce na to, aby osobní údaje umožňující identifikaci subjektů údajů byly uloženy pro dané účely zpracování pouze po nezbytně nutnou dobu, s výjimkou účelů archivace ve veřejném zájmu a pro statistické účely nebo účely výzkumného a historického výzkumu. Není-li možné tuto dobu zcela jasně určit, měl by správce být schopen doložit kritéria, která stanovil k určení této lhůty stanovil. To se týká například zdravotnické dokumentace, kdy se údaje v nemocnicích uchovávají do doby úmrtí pacienta, někdy i po této době.

f) Zásada integrity a důvěrnosti

U této zásady skládající se ze dvou atributů prakticky hovoříme o neporušenosti a celistvosti osobních údajů (integritě), a také o zabezpečení při manipulaci

s nimi, včetně přístupu odpovědných osob k těmto údajům (důvěrnosti). V zákoně o kybernetické bezpečnosti se podle § 2 písm. d) rozumí „*bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací a dat*“. Kybernetická bezpečnost se tak s ochranou osobní údajů vzájemně doplňují.

4.2.5 Pověřenec

Pověřenec pro ochranu osobních údajů (dále jen „pověřenec“) je profesní označení, které přišlo spolu s Obecným nařízením. Označuje se také pod anglickou zkratkou DPO, což znamená „*Data Protection Officer*“, a je zakotven v čl. 37 až 39 Obecného nařízení. Předmětné články pak uvádí, co obnáší proces jmenování pověřence, jaké je jeho postavení v instituci, a jaké jsou jeho úkoly. Jedná se o základní souhrn, který bývá upřesňován různými metodickými příručkami. Například Ministerstvo vnitra České republiky připravilo „*Metodické doporučení k problematice pověřenců pro ochranu osobních údajů ve služebních úřadech*“[32]. Další dostupné informace podává prostřednictvím svých webových stránek rovněž ÚOOÚ[33], kde lze například získat užitečné „*Pokyny týkající se pověřenců pro ochranu osobních údajů*“ vydané Pracovní skupinou WP29 (viz kapitola 4.2.6) a přijaté dne 13. prosince 2016, po poslední revizi přijaté dne 5. dubna 2017. Pověřenec by pak měl být osobou s dostatečnými odbornými znalostmi v dané problematice a být nápomocen správci nebo zpracovateli při sledování souladu s Obecným nařízením a ZoZOÚ ve vztahu k vnitropodnikové dokumentaci správce, a tím také chránit zájmy subjektů údajů, analyzovat rizika zpracování ve spolupráci se správcem a předkládat správci posudky k provedeným posouzením vlivu (pokud jsou). Jednou z činností je také zvyšování povědomí zaměstnanců v souvislosti s ochranou osobních údajů a poskytování poradenské a konzultační činnosti správci při různých operacích zpracování.

---

[32] Pověřenec pro ochranu osobních údajů - Ochrana osobních údajů. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2022 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 07.08.2022]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/poverenec-pro-ochranu-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju.aspx

[33] Pověřenec pro ochranu osobních údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 07.08.2022]. Dostupné z: https://www.uoou.cz/poverenec%2Dpro%2Dochranu%2Dosobnich%2Dudaju/ds-5550/p1=5550

Pro státní instituce je povinnost jmenovat pověřence uvedena jednak v čl. 37 odst. 1 písm. a) Obecného nařízení, a dále také v ust. § 14 ZoZOÚ, které doplňuje, že tato povinnost se ukládá pro orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu. Pověřenec je osoba většinou přímo odpovědná vedoucímu celého úřadu. V některých případech bývá pro pověřence zřízeno také samostatné oddělení, kdy má pod sebou další zaměstnance plnící činnosti v této oblasti. Občasným nešvarem bývá, že i když je pověřenec jmenován, často mu chybí dostatečná informovanost o činnostech, které v organizaci probíhají, a které se týkají ochrany osobních údajů. Na úkor toho bývá pověřenec postaven mimo hlavní dění a některé záležitosti týkající se ochrany osobních údajů se k němu dostávají až v čase, kdy je řešení urgentní nebo je nutné provádět nápravu nežádoucího stavu.

4.2.6 Sbor pověřenců

Před příchodem Obecného nařízení se v tomto kontextu hovořilo o „Pracovní skupině WP29“, která zkráceně označovala Pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, jež vycházela z čl. 29 Směrnice 95/46/ES. Její úkoly byly popsány v čl. 30 této směrnice, a rovněž v čl. 15 Směrnice o soukromí a elektronických komunikacích (viz kapitola 2). S nástupem Obecného nařízení došlo ke změně na Evropský sbor pro ochranu osobních údajů, vedený též pod anglickou zkratkou EDPB, tedy „*European Data Protection Board*“ (dále jen „Sbor pověřenců“), který je definován jako „*nezávislý evropský subjekt, který přispívá k jednotnému uplatňování pravidel ochrany údajů v celé Evropské unii a prosazuje spolupráci mezi úřady pro ochranu osobních údajů v EU*“[34]. Tím je v podstatě sdělen cíl jeho pracovního snažení. Jeho úkolem je zejména osvěta a metodická podpora v oblasti ochrany osobních údajů poskytovaná prostřednictvím vydávaných pokynů. Tyto pokyny jsou podkladovými materiály, které by měly objasnit nebo upřesnit jednotlivé části Obecného nařízení, zajistit jednotnost při uplatňování jeho pravidel a zlepšit jeho výklad nebo implementaci procesních postupů. Neméně důležitou součástí je

[34] Kdo jsme | European Data Protection Board [online]. [cit. 06.08.2022]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_cs

také spolupráce v této oblasti při výměně informací a poznatků z praxe, které mohou zprostředkovat zástupci dozorových úřadů, kteří tvoří spolu se zástupci Evropského inspektora ochrany osobních údajů Sbor pověřenců[35]. Pro další informace o Sboru pověřenců lze nahlédnout na čl. 68 až 76 Obecného nařízení. Informace o vydávaných pokynech pak uveřejňuje například Dozorový úřad[36], kde je rovněž odkaz na příslušné webové stránky. Pověřenec pro ochranu osobních údajů ustanovený v příslušné státní instituci by měl tyto pokyny sledovat a dbát na jejich dodržování, jsou-li pro činnost instituce relevantní.

4.2.7 Zabezpečení osobních údajů

Zabezpečení osobních údajů je jednou z povinností, které správce musí plnit. Obecné nařízení sice přihlíží pro praxi zcela jistě užitečně také k technickým a finančním možnostem správce, nicméně není vždy možné plnit Obecné nařízení bez určitých inovací nebo technického zhodnocení, leč jsou někdy náklady na zabezpečení bohužel přednější než zabezpečení samotné. Zabezpečení zpracování pak rozvádí čl. 32 Obecného nařízení, kde se uvádí, že správce nebo zpracovatel provedou vhodná technická a organizační opatření (viz kap. 4.3.3), aby zajistili úroveň zabezpečení odpovídající danému riziku, včetně: „pseudonymizace a šifrování osobních údajů; schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování; schopnosti obnovit dostupnost osobních údajů a včasný přístup k nim po fyzickém nebo technickém incidentu; procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených techn. a organ. opatření pro zajištění zabezpečení zpracování“, a to s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a závažným rizikům pro práva a svobody fyzických osob. Při posuzování vhodné úrovně zabezpečení se pak zohledňují zejména rizika, která by mohla způsobit zničení, ztrátu, pozměnění, neoprávněné

[35] Kdo jsme | European Data Protection Board [online]. [cit. 06.08.2022]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_cs

[36] Pokyny evropského Sboru (EDPB): Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.08.2022]. Dostupné z: https://www.uoou.cz/pokyny%2Devropskeho%2Dsboru%2Dedpb/ds-4728/p1=4728

zpřístupnění nebo jiné neoprávněné či protiprávní zpracování osobních údajů. Výše uvedené by měl správce zabezpečit v rámci svých možností, a vést o tom příslušnou dokumentaci. Pokud by správcem nebo zpracovatelem byla za zpracování pověřena určitá osoba, pak bude při zpracování údajů jednat pouze na základě pokynů správce nebo zpracovatele, neukládá-li ji zpracování přímo právní řád České republiky nebo právo EU (čl. 32 odst. 4 Obecného nařízení).

4.2.8 Porušení zabezpečení osobních údajů

Správce je rovněž povinen ohlásit nebo oznámit porušení zabezpečení osobních údajů, a to jak dozorovému úřadu, tak i subjektu údajů. Jsou zde ovšem výjimky, kdy toto není potřeba. Proto je potřeba si říci, kdy tato povinnost je aktuální, a kdy naopak být naplněna nemusí. Tyto povinnosti upravuje čl. 33 (ohlášení dozorovému úřadu) a čl. 34 (oznámení subjektu údajů) Obecného nařízení.

Ohlašovat je potřeba jakékoli porušení zabezpečení osobních údajů, které může mít za následek vysoké riziko pro práva a svobody fyzických osob. Takové oznámení by mělo být učiněno do 72 hodin od okamžiku, kdy se o něm správce dozvěděl. K ohlášení není nutné přistoupit, pakliže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody dotčených osob. Co do obsahových náležitostí by mělo zahrnovat informace uvedené v čl. 33 odst. 3 Obecného nařízení, anebo dostupné na stránkách dozorového úřadu[37]. Oznamovat je zase potřeba bez zbytečného odkladu takové porušení, u kterého je pravděpodobné, že bude mít za následek vysoké riziko pro práva a svobody fyzických osob. Oznámení se však nevyžaduje tehdy, zavedl-li správce náležitá technická a organizační opatření, která aplikoval u předmětných údajů, anebo přijal následná opatření k zajištění mitigace předchozího rizika, popř. pokud by to vyžadovalo nepřiměřené úsilí, avšak v tom případě je nutné informovat subjekt údajů jiným, stejně účinným způsobem. Dále toto porušení také rozvádí například recitál 85 Obecného nařízení, který uvádí další doplňující informace.

[37] Ohlašování případů porušení zabezpečení: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 30.08.2022]. Dostupné z: https://www.uoou.cz/ohlasovani-pripadu-poruseni-zabezpeceni/d-30181

4.3 Vnitropodniková dokumentace

Každý příslušný orgán státní správy, který je v roli správce při zpracování osobních údajů, je povinen vést příslušnou dokumentaci a pravidelně ji aktualizovat. K tomu má, anebo by měl mít, interní prováděcí dokument (vnitřní předpis), nejčastěji v podobě příkazu či směrnice. Tento vnitřní předpis upřesňuje postup orgánu při zpracování osobních údajů a stanoví vhodná technická a organizační opatření k zajištění jejich ochrany. Samotná dokumentace k ochraně osobních údajů pak tvoří ucelený soubor, který odpovídá požadavkům kladenými právními předpisy. Příslušnou dokumentaci musí vést také zpracovatel a správce by měl mít možnost pravidelných kontrol. Správce může také vytvořit své formuláře v rámci informační povinnosti podle čl. 12 Obecného nařízení, jejich využití ovšem není vyžadováno. Chceme-li však zajistit naplňování Obecného nařízení, nejde to uskutečnit bez toho, aniž bychom v instituci neměli implementovány také směrnice a normy pojednávající o bezpečnosti informací a dat, které jsou často součástí komplexnějšího integrovaného systému řízení organizace, pod který spadá také systém řízení bezpečnosti informací. V první řadě je samozřejmě nejdůležitější směrnice zabývající se ochranou a zpracováním osobních údajů. Dále je pak ale důležitá také směrnice, která se bude zabývat bezpečností informačních technologií, systémem řízení bezpečnosti informací, bezpečnostní politikou ICT v organizaci, fyzickou bezpečností nebo personální bezpečností. Důležitý je samozřejmě také provozní řád ICT nebo spisový řád. Samotná ochrana osobních údajů pak může být promítnuta přímo i nepřímo v jiných vnitropodnikových směrnicích a pokynech. Zpravidla se v jednom či více bodech objevuje například v etickém kodexu. Správce má samozřejmě také povinnost veřejně informovat o ochraně osobních údajů a jak k ní přistupuje, což zajišťuje také opatřeními v uzavíraných smlouvách s dodavateli, ve kterých je tato otázka bezpečnosti rovněž řešena. To vše musí mít ovšem nastaveno ve svých vnitropodnikových procesech, bez nichž by komplexnější zabezpečení ochrany osobních údajů nebylo možné, anebo zcela jistě do značné míry alespoň komplikované.

4.3.1 Vnitřní předpis

Tento dokument obecně definuje naplnění výkonu činnosti související s ochranou osobních údajů v prostředí správce (státní instituce). Zároveň také uvádí právní předpisy, kterými se při výkonu své činnosti řídí (zejména se jedná o legislativu vymezenou v kapitole č. 2 této práce). Základním právním dokumentem zůstává Obecné nařízení následované ZoZOÚ. Další předpisy, pokud jsou uvedeny, se mohou lišit podle předmětu vykonávané činnosti v příslušné státní instituci. Dále jsou uvedeny základní pojmy a procesní postupy, včetně realizace práv subjektu údajů. Mohou být také upřesněny povinnosti vedoucích zaměstnanců a zaměstnanců při procesu zpracování a nakládání s osobními údaji, případně při porušení zabezpečení osobních údajů. Takový dokument má zároveň zajistit jednotnost v postupu napříč státní institucí, a to v souladu se základními zásadami při zpracování (viz kap. 4.2.4). Dokument může dále pojednávat o zpracování osobních údajů zpracovatelem nebo o zajištění technických a organizačních opatření a jejich náležitostech, dále o kamerovém systému, o manipulaci s osobními údaji při jejich přepravě, o provádění kontrol, o výmazu či zničení osobních údajů, a také o postupech při narušení zabezpečení ochrany osobních údajů či o odpovědnosti zaměstnanců.

4.3.2 Záznamy o činnostech zpracování

Jedním z klíčových dokumentů, který by neměl chybět u žádného správce osobních údajů, jsou záznamy o činnostech zpracování, za něž je správce nebo jeho zástupce plně odpovědný, a měl by provádět jejich pravidelnou aktualizaci. Záznamy o činnostech zpracování nalezneme primárně v čl. 30 Obecného nařízení. Tyto záznamy slouží k doložení souladu s nařízením, a to jak pro správce, tak případně také pro zpracovatele (recitál 82 nařízení). Oba uvedení by pak měli být schopni na základě požadavku od dozorového úřadu tento materiál předložit z důvodu jejich analýzy se skutečným stavem (čl. 30 odst. 4 nařízení). Záznamy o zpracování je potřeba vyhotovit jak v písemné, tak elektronické podobě (čl. 30 odst. 3 nařízení). Zda budoucí správce stanoví vykonávané agendy nebo bude upřednostňovat zpracování podle jednotlivých oddělení či odborů je už věcí interní domluvy. Důležitá je pak konzistentnost

takového zpracování a zajištění pravidelného informování o změnách, které proběhly na některém z úseků nebo pracovišti, aby byly promítnuty do zpracovaných záznamů. V závislosti na objemu dokumentace někdy může být výhodnější zvolit zaslání formuláře v podobě ohlášení změny, který bude přiložen ke stávající dokumentaci pod předmětnou agendu či pracoviště. Obsahové náležitosti stanovené v čl. 30 nařízení pak vymezují základ toho, jaké informace by měly předmětné záznamy obsahovat (viz níže).

1. Záznam o činnosti zpracování správcem
   a) Jméno a kontaktní údaje správce, společného správce a/nebo jmenovaného zástupce správce a pověřence pro ochranu osobních údajů
   b) Účely zpracování
   c) Popis kategorií subjektů údajů a kategorií osobních údajů
   d) Kategorie příjemců, kteří mají k údajům přístup, včetně příjemců, kteří jsou mimo EU (třetí země a mezinárodní organizace)
   e) Detailní informace o předání osobních údajů do třetích zemí či mezinárodních organizací, včetně jejich identifikace a doložení vhodných záruk v případě uskutečnění předání
   f) Lhůta pro výmaz jednotlivých kategorií osobních údajů
   g) Obecný popis technických a organizačních opatření navazujících na čl. 32 odst. 1 (viz také kap. 4.2.7)
2. Záznam o činnosti zpracování zpracovatelem
   a) Jméno a kontaktní údaje zpracovatele a každého správce, jehož jménem zpracovatel jedná (zpracovává osobní údaje), případně jmenovaného zástupce správce nebo zpracovatele a pověřence
   b) Kategorie zpracování vykonávaných pro každého správce
   c) Detailní informace o předání osobních údajů do třetích zemí či mezinárodních organizací, včetně jejich identifikace a doložení vhodných záruk v případě uskutečnění předání
   d) Obecný popis technických a organizačních opatření v oblasti bezpečnosti

4.3.3 Technická a organizační opatření

Druhým neméně důležitým materiálem, který správce či zpracovatel eviduje v souvislosti s dokumentací k ochraně osobních údajů, jsou technická a organizační opatření. Obecné nařízení není v tomto ohledu co do výčtu zcela vyčerpávající, a proto spíše naťukává co vše by mohlo nebo mělo být do těchto opatření zaneseno. Prvotní informace poskytuje v čl. 32 v rámci zabezpečení zpracování (viz kap. 4.2.7) a v zajištění dostatečné úrovně odpovídající případnému riziku, a to včetně například zabezpečení pomocí pseudonymizace. Jak již bylo krátce zmíněno v kapitole 4.2., na anonymizovaná data se Obecné nařízení nevztahuje. Rozdíl mezi pseudonymizací a anonymizací osobních údajů spočívá v tom, že při pseudonymizaci je možné následně data opět přiřadit k určité osobě, která je jejich vlastníkem (resp. nositelem dané informace). Při anonymizaci dochází ke kompletnímu zapomenutí subjektu údajů, a tím také ke smazání či likvidaci osobních údajů spojených s konkrétní osobou, čímž se předpokládá, že tato data či záznamy přestávají existovat[38]. Důležité je však poznamenat, že prostřednictvím moderních nástrojů lze docílit i obnovy již smazaných dat. Proto je vhodné se k zařízení nebo nástroji s datovým úložištěm i po smazání dat chovat tak, jako by tam stále tato data byla uložena. Rovněž je potřeba mít správně nastaven vnitropodnikový proces likvidace těchto zařízení či nástrojů pro uchování dat.

Jak již bylo dříve uvedeno, součástí technických a organizačních opatření by mělo být také zajištění:

a) pseudonymizace a šifrování osobních údajů
b) kontinuity u důvěrnosti, integrity, dostupnosti, a odolnosti systémů a služeb zajišťujících zpracování
c) schopnosti obnovit oprávněně zpracovávané osobní údaje a přístup k nim v případě fyzických nebo technických incidentů
d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření

[38] Anonymizace a pseudonymizace jsou dvě rozdílná slova | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. [cit. 06.08.2022]. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/

Veškerá technická a organizační opatření sloužící k zajištění ochrany osobních údajů by měla být v dané státní instituci prováděna v souladu s vydaným závazným dokumentem k ochraně osobních údajů, dále v souladu s právními předpisy, a také s vnitropodnikovou dokumentací (směrnice, nařízení, pokyny). Nemělo by poté dojít k situacím, kdy by hrozilo neoprávněné nebo nahodilé zpracování či přístup k osobním údajům, obdobně ani k jejich pozměnění, ztrátě nebo zničení. Tyto povinnosti platí rovněž po ukončení zpracování. Samotný výstupní dokument, který lze obecně pro účely této práce nazvat zdokumentování technických a organizačních opatření k zajištění ochrany osobních údajů, by pak mohl či měl, nikoli však nutně obligatorně v celém svém rozsahu, obsahovat následující informace nebo body.

1) Úvodní strana obsahující název státní instituce, její adresu, příslušný útvar, číslo jednací, jméno zpracovatele a schvalovatele, datum vydání s podpisy odpovědných osob, případně číslo nebo počet výtisků a příloh
2) Specifikaci zpracování osobních údajů zahrnující účel zpracování (definovat účel a případně zahrnout příslušné právní předpisy), prostředky a způsob zpracování (například osobní počítač a mzdový software, listinná nebo elektronická podoba), kategorie osobních údajů (jaké údaje jsou zpracovávány, například, jméno, titul, adresa bydliště, ad.) a subjektů údajů (tj. k jakým subjektům údajů se vztahují, například zaměstnanci, uchazeči o zaměstnání), shromažďování údajů (jakým způsobem jsou údaje získávány a z jakých zdrojů), místo nebo místa zpracování (kde dochází ke zpracování) a příjemce nebo kategorie příjemců (uvést, zda jsou údaje předávány jiným subjektům, pokud ano, tak jaké a komu, a zda údaje putují do dalších zemí)
3) Opatření k ochraně osobních údajů zahrnující technická a organizační opatření, přičemž:
    a. Organizační opatření budou zahrnovat práva, povinnosti a odpovědnost osob, povinnost mlčenlivosti (upravena většinou vnitřním předpisem a smluvně se zaměstnanci), školení zaměstnanců (dkdo zajišťuje a provádí, jak často, jakou formou), kontrolní činnost (kdo zajišťuje a provádí, jaké záznamy o tom zpracovává, jak často a v jaké formě), relevantní dokumentaci (jaká dokumentace je vedena

v souvislosti se zajištěním ochrany osobních údajů) a posouzení rizik (způsob, jakým byla posouzena rizika související se zpracováním)

b. Technická opatření a související režimová opatření zahrnující způsoby zajištění ochrany osobních údajů v rámci areálu (střežení kamerovým systémem, uzamykací systém, kontrola vjezdu), objektu (monitoring kamerovým systémem, kontrola vstupu, elektrický zabezpečovací systém, elektrický požární systém), kanceláří (umístění těch, kde dochází ke zpracování, případně mříže u oken, zabezpečení přístupu), prostředků zpracování (ukládání spisů v uzamykatelných skříních, kdo má duplikáty klíčů, software pro zpracování, napojení vnějších sítí na počítačový systém) a fyzické ostrahy (rozsah a způsob zajištění ostrahy v místních podmínkách)

Odstavec č. 3 neposkytuje ucelený výčet všech možných opatření, ale pouze nástin různých prvků, které bývají uváděny. O něco šířeji se náležitosti technických a organizačních opatření dají členit na administrativní opatření, režimová opatření, fyzickou ostrahu, fyzickou bezpečnost a bezpečnost informačního systému. Vnitropodnikový předpis k ochraně osobních údajů může tato opatření buď rozvést, anebo v rámci bodu vztahujícího se k tomuto tématu odkázat na příslušné další interní předpisy, ve kterých jsou tato opatření dále rozpracována.

4.3.4 Posouzení rizika

Posouzení rizika se do jisté míry prolíná se zabezpečením zpracování, kdy může hrozit riziko pro práva a svobody fyzických osob (tím může být například spojování či propojování různých databází původně shromážděných pro více účelů nebo různými správci[39]). Například u poskytovatelů cloudových služeb by měl správce požadovat záruky, že data uložená na úložišti nebudou přístupná jiným subjektům, kterým správce poskytuje v rámci svých služeb své datové prostory. Tyto prostory musí být odděleny a nesmí dojít k jejich konfliktu.

[39] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 124.

Samotné posouzení rizika by měl správce učinit v případech, kdy zpracování není podle právního nebo smluvního aktu, a hrozí zároveň riziko v oblasti narušení důvěrnosti, integrity nebo dostupnosti osobních údajů. Správce zde identifikuje a hodnotí hrozby spojené se zpracováním, a dále identifikuje potenciální újmu, ke které by mohlo dojít. Takovýmto posouzením může být následně ověřena případná nesourodost zpracování se zásadami zpracování (viz kap. 4.2.4). Obecné nařízení pak pojednává o rizicích spojených se zpracováním například v recitálu 15 (ochrana fyzických osob by se měla vztahovat jak na automatizované zpracování osobních údajů, tak na manuální zpracování), 76 (pravděpodobnost a závažnost rizika pro práva a svobody subjektu údajů by měly být určeny na základě povahy, rozsahu, kontextu a účelům zpracování, zároveň riziko by mělo být hodnoceno na základě objektivního posouzení, které stanoví, zda operace zpracování představují riziko či vysoké riziko) nebo 83 (v zájmu zachování bezpečnosti a zabránění zpracování, které by bylo v rozporu s tímto nařízením, by měl správce nebo zpracovatel posoudit rizika spojená se zpracováním a přijmout opatření ke zmírnění těchto rizik, například šifrování). Podmínky přesně vymezující obsahové náležitosti dokumentace nebo postup k určení rizika v Obecném nařízení nedohledáme. Vhodným nástrojem může být proto také aplikace normy ISO/IEC 27005, která stanovuje řízení rizik bezpečnosti informací. Návrh, jak se určí riziko porušení zabezpečení podává například dozorový úřad v bodě č. 8 pojednávajícím o zabezpečení osobních údajů, a je citováno v odstavcích níže[40].

„*Při určování rizika porušení zabezpečení bude nutné vycházet zejména z kategorie osobních údajů, které byly porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtem dotčených subjektů údajů. Vyšší riziko budou vždy představovat zvláštní kategorie osobních údajů (např. údaje o zdravotním stavu), případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv (např. únik přihlašovacích údajů do elektronického bankovnictví).*“

[40] Základní příručka k ochraně údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/zakladni-prirucka/ds-4744/p1=4744

„Dalším rozhodným prvkem může být i okolnost, zdali došlo k porušení zabezpečení úmyslně či nedbalostně, přičemž úmyslný čin výrazně zvyšuje riziko takového činu, jelikož osobní údaje byly terčem útoku. Porušení zabezpečení se tak musí provést komplexně, nikoli izolovaně a vyšlé riziko následně určí eventuální povinnost oznámit porušení zabezpečení Úřadu nebo i oznámit subjektu údajů.“

4.3.5 Posouzení vlivu a balanční test

Posouzení vlivu na ochranu osobních údajů a balanční test jsou dva důležité pojmy, které je od sebe však potřeba rozlišovat. Zatímco v prvním případě můžeme hovořit o posouzení, při kterém hodnotíme dopad určitého druhu zpracování na práva a svobody osob, u balančního testu hodnotíme legitimitu takového zpracování. Státní instituce nebudou pravděpodobně příliš často tyto prvky využívat, a pokud ano, pak na základě čl. 6 odst. 1 písm. f) Obecného nařízení, což se může dotýkat například kamerového systému (viz kap. 4.5). Posouzení vlivu, zkráceně také DPIA (Data Protection Impact Assessment) více rozvádí čl. 35 Obecného nařízení, anebo recitál 84 tohoto nařízení. Pokud přeci jen bude státní instituce provádět posouzení vlivu, je přinejlepším vhodné použít jako podkladový materiál Metodiku obecného posouzení vlivu na ochranu osobních údajů, aktuálně ve verzi 1.0 ze dne 11. listopadu 2020[41], včetně překontrolování seznamu operací, při kterých je, anebo není nutné takové posouzení provádět[42]. Další podrobnosti může poskytnout například odborná literatura[43]. Balanční test se naproti tomu týká otestování proporcionality u oprávněnosti zpracování (tedy u oprávněného zájmu). Pakliže povinnost zpracování vyplývá ze zákona nebo smlouvy, není potřeba balanční test provádět. V opačném případě by byl potřeba, ovšem státní instituce většinou zpracovávají osobní údaje ze zákonných důvodů (tj. na základě právního titulu).

---

[41] Posouzení vlivu na ochranu osobních údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/posouzeni-vlivu-na-ochranu-osobnich-udaju/ds-6413/p1=6413

[42] Tamtéž

[43] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 121 až 127.

4.3.6 Diferenciace dokumentace

Dokumentace k ochraně osobních údajů by měla odpovídat požadavkům kladeným na správce Obecným nařízením. Každá instituce však může mít dokumentaci nastavenu trochu odlišně, mít jinou formu zpracování, řídí se jinými podmínkami, za kterých osobní údaje zpracovává. Obecně se vyžadují například technická a organizační opatření (a to i pro kamerový systém) nebo záznamy o činnostech zpracování, jejichž minimální rozsah je nařízením vymezen, ovšem finální realizace bude podléhat kontextu organizace a do jisté míry také lidové tvořivosti. Mezi dalšími dokumenty, které se mohou objevit jako součást dokumentace k ochraně osobních údajů nebo jako příloha k interní směrnici, jsou níže uvedené příklady. Je samozřejmě možné, že při zpracování mohou být některé materiály a informace slučovány nebo vypuštěny.

a) Katalog operací
b) Prohlášení o souhlasu s použitím fotografie
c) Posouzení nezbytnosti zpracování
d) Formulář pro hlášení změn
e) Formulář k informaci o plnění povinností vyplývajících z vnitropodnikové směrnice o ochraně osobních údajů
f) Stanovený harmonogram kroků pověřence (spíše informativní)
g) Katalog osobních údajů
h) Formulář pro určení rizikovosti zpracování či posouzení vlivu
i) Povinnost zachovávat mlčenlivost
j) Výjimky zákazu zpracování osobních údajů (spíše informativní)
k) Formulář pro souhrn práv subjektu údajů a právního titulu zpracování (spíše informativní)
l) Formulář pro vyřizování žádostí od subjektů údajů (spíše informativní)
m) Formulář pro hlášení incidentu
n) Formulář k oznamovací povinnosti o porušení zabezpečení
o) Záznamy o provedených kontrolách v rámci výkonu agendy
p) Zpráva o výsledku kontroly vedoucím zaměstnancem
q) Vyhodnocení plnění povinností správce
r) Vzorové označení a formulář ke kamerovému systému

4.4 COVID-19

S příchodem koronavirového onemocnění bylo v průběhu času vydáno Ministerstvem zdravotnictví mimo jiné také mimořádné opatření pod č.j. MZDR 47828/2020-16/MIN/KAN ze dne 1. března 2021, kterým bylo nařízeno povinné testování zaměstnanců v podnicích na území České republiky, následované mimořádným opatřením č.j. MZDR 9364/2021-1/MIN/KAN ze dne 5. března 2021 týkající se testování u veřejných zaměstnavatelů. Dlužno dodat, že úderem tohoto pomyslného kladiva na čarodějnice, jak by se s jistou nadsázkou dalo říci, byla agenda ochrany osobních údajů vystavena další tvrdé zkoušce. Přibyla totiž nová agenda zpracování, která musela být promítnuta do záznamů o činnostech zpracování (viz kap. 4.3.2), a také nové, do té doby netušené výzvy.

Rovněž v mnoha orgánech státní správy přibyla nová kategorie osobních údajů, a to kategorie související s údajem o zdravotním stavu. Zavedení opatření v těchto orgánech se samozřejmě v některých ohledech lišilo. Přímo řízené organizace spadající pod působnost jednotlivých ministerstev se často řídily právě tím, jak k tomu přistupovaly tyto ústřední správní orgány a snažily se leckdy přejímat jejich nápady, ať už dobré, anebo i ty špatné. Důležité také bylo, v jaké kvalitě se ochrana osobních údajů v jednotlivých orgánech vykonávala, případně jak se k tomu povedlo organizačně či technicky přistoupit. Zaměstnavatelé byli povinni zajistit, aby zpracování osobních údajů bylo prováděno s co možná nejvyšší mírou ochrany soukromí, vést příslušnou evidenci testovaných osob a řádně ji zabezpečit, pověřit odpovědné osoby k zajištění úkonů zpracování a omezit přístup jiných neoprávněných osob. Doba uložení osobních údajů byla stanovena nejprve na dobu nezbytně nutnou k doložení zákonného jednání správce (tj. do zrušení mimořádného opatření k provádění testování), posléze byla maximální doba uchování osobních údajů, včetně evidence provedených testů stanovena na 3 roky od doby jejich pořízení. Subjekt údajů byl povinen poskytnout své osobní údaje za účelem splnění povinnosti zaměstnavatele vyplývající pro něj z mimořádného opatření, správce musel naopak podat informační povinnost a práva subjektu údajů mohla být plněna kromě práva odvolat souhlas a práva na přenositelnost. Žádoucí bylo

samozřejmě také dodržet zásadu minimalizace, což ovšem někdy bylo komplikované například kvůli nejasným informacím o způsobu proplácení testů a možném vedení čísel pojištěnců (ve většině případů rodných čísel). Informovanost zaměstnavatele v případě pozitivního (ale také negativního) testu pak měla být s ohledem na citlivé informace omezena pouze na odpovědné osoby. Zda tomu tak skutečně bylo, je však pouze v dobré víře.

4.5 Kamerový systém

V dnešní době neustálého rozvoje informačních a komunikačních technologií se rozvíjí také vlastnosti obrazových sledovacích zařízení, na které jsou kladeny stále větší požadavky, a to jak na kvalitu pořizovaného materiálu, technickou vybavenost a účelovost, tak i na bezpečnost při manipulaci s touto technikou a s nakládáním pořízeného materiálu. Kamerové systémy, mezi které lze zařadit také určité typy fotopastí, slouží svým pořizovatelům pro různé účely. Jedním z nich je ochrana osob a majetku. Tato kapitola je především určitým pojednáním o kontinuitě mezi kamerovým systémem a ochranou osobních údajů, a to především z pohledu správce osobních údajů.

Pokud hovoříme o kamerových systémech, je ve známosti obecné označení CCTV (tzv. uzavřený televizní okruh), neboli „Closed Circuit Television System". Jedná se o „*systém sestávající z kamerového zařízení, monitorovacího a přidruženého zařízení pro přenosové a řídící účely, které mohou být nezbytný pro dohled nad chráněným prostorem*"[44]. Odbornějším označením, pod které spadá také CCTV, je VSS (tzv. dohledový videosystém), neboli „Video Surveillance System". Zde se jedná o „*systém skládající se z kamerového vybavení, úložiště, monitorovacího a souvisejících zařízení pro účely přenosu obrazu a ovládání*"[45]. Tyto definice vyplývají z konkrétních norem ČSN, konkrétněji pak ČSN EN 62676-4 a ČSN EN 62676-1-1.

[44] Kamerové systémy - TZB-info: *Kamerové systémy* [online]. Topinfo s.r.o., Copyright © 2001-2021 [cit. 24.8.2022]. Dostupné z: https://www.tzb-info.cz/kamerove-systemy
[45] Tamtéž

Kamerový systém tvoří v dnešní době jeden ze základních prvků při zajišťování bezpečnosti, a to jak z pohledu včasné reakce na protiprávní jednání, tak i z pohledu budoucího poskytování součinnosti orgánům činným v trestním řízení, případně správnímu orgánu při projednávání přestupku. V rámci této práce se jedná především o kamerové systémy střežící důležité objekty státních institucí (sídla úřadů, objekty značné hodnoty z důvodu uložených zásob či materiálu v objektu, objekty historické hodnoty, zákonná povinnost, ad.), ale může být fakticky použitelná i pro jiné typy organizací. Při instalaci je nutné předem zjistit a posoudit veškeré prvky objektové bezpečnosti, které jsou na místě, a zvážit nutnost zavedení nebo provozování takového systému. Je však nutné také zmínit, že z pohledu ochrany osobních údajů u kamerového systému existuje mnoho úskalí.

Problematika kamerového systému, zejména kamerového systému se záznamem, je z pohledu ochrany osobních údajů důležitým faktorem, ke kterému je nutné přistupovat obezřetně, a to jak z pohledu práv zaměstnanců, tak i dalších osob, které jsou tímto monitoringem dotčeny. Kamerový systém bylo v minulosti nutné také registrovat u dozorového úřadu za pomoci registračního formuláře, který byl dříve součástí povinné registrace podle § 16 ZoOOÚ. Základním předpisem v oblasti ochrany osobních údajů, který postihuje jejich zpracování kamerovým systémem a má na kamerový systém dopad, je opět Obecné nařízení, následované také ZoZOÚ. Rozpracování konkrétních požadavků Obecného nařízení na provoz kamerového systému je rovněž obsaženo v dokumentu „*Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky*“[46], který vydal Sbor pověřenců (kap. 4.2.6). Pokyny a doporučení k provozu kamerového systému pro splnění základních povinností ukládaných právními předpisy v předmětné oblasti rovněž vydává dozorový úřad, tedy Úřad pro ochranu osobních údajů (viz kap. 4.6).

[46] Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky | European Data Protection Board [online]. [cit. 24.08.2022]. Dostupné z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-thro-ugh-video_cs

Při zajišťování potřeb pro plnění povinností vyplývajících z Obecného nařízení je nutné počítat i s negativními vlivy, za které lze považovat například problematické řešení spoluvlastníků u objektu snímaného kamerovým systémem, neochota komunikace při šetření celkového stavu systému, nedostatečné vyjasnění provozovatele kamerového systému, chybná či nedostatečná nebo zcela chybějící projektová dokumentace ke kamerovému systému (což může mít za následek, že není zřejmé, kudy vedou elektrické obvody a jak přesně je řešen svod kamerového systému k příslušným záznamovým zařízením), záběr zorného (snímatelného) úhlu kamerového systému a v neposlední řadě také omezení funkčnosti systému z důvodu končící nebo již ukončené životnosti takového systému. Na pomyslný piedestal pak už lze umístit jen chybějící servisní smlouvu a s tím související neuskutečňované revize. Negativním vlivem mohou být také nesprávné zásahy do interních systémů instituce, které naruší chod kamer, anebo samotný charakter budovy.
Z pohledu ochrany osobních údajů mohou dále nastat například následující dvě situace k řešení. První z nich je stav, kdy kamerový systém nebo fotopasti nejsou na místě instalovány a projednává se zavedení takového opatření, s čímž souvisí i dodržování různých pravidel. Další možností je stav, kdy kamerový systém je již instalován, ale je potřeba opatřit příslušnou dokumentaci, popř. její aktualizaci a doplnění. V obou případech bude potřeba vyjasnit, charakterizovat a zaznamenat konkrétní podmínky fungování systému, které jsou popsány v následujících odstavcích níže.

Stanovit účel ochrany budovy pro provozování kamerového systému nebo fotopastí[47]. Takovým účelem může být v daném případě např. ochrana majetku. Je nutné však předem zhodnotit, zda není případně možné využít jiného, méně invazivního prostředku. S tím souvisí také vyhodnocení ekonomických dopadů a rizik spojených s nákupem a provozem kamerového systému nebo fotopasti při zjišťování bezpečnostních opatření, která jsou pro předmětný objekt již realizována. Například jedná-li se o objekt ve správě určitého orgánu nebo

[47] Čl. 5 odst. 1 písm. b) Obecného nařízení: „*Osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný*“.

instituce, pak je vhodné se ptát, zda tam zaměstnanci instituce dochází pravidelně, anebo zda podléhá pouze občasné kontrole (např. technické), při které je případně zjištěno možné narušení zabezpečené oblasti. Každý správce si musí vyhodnotit důležitost zabezpečení příslušného aktiva a potřebné náklady.

Dále nás zajímá, co se případně v objektu skladuje nebo jaké činnosti tam kdo vykonává. Takové osoby musí být seznámeny s provozem kamerového systému v oblasti. Toto se částečně koriguje u fotopastí, u kterých by ani běžní zaměstnanci neměli vědět jejich přesné umístění. Pakliže by jejich umístění znali, mohl by být ohrožen účel, pro který tam byly umístěny. V případě kamer není možné toto vždy ovlivnit už z povahy věci, kdy osoba může vykonávat funkci dozoru u monitoru poskytujícího videopřenos. Ve všech případech je však nutné zajistit označení pro provoz kamerového systému, a to buď se záznamem nebo bez záznamu. Pro kamerový systém se záznamem musí být vyplněna širší dokumentace. U kamerového systému bez záznamu je zásadní povinností viditelné umístění označení popisující tuto skutečnost subjektům údajů. S tím opět souvisí úprava konkrétních vlastností pořizovaného nebo již instalovaného zařízení. Také zde je potřeba předem určit a vymezit, co konkrétně ze všech vlastností daného zařízení bude skutečně využíváno, resp. následně provozováno, a rovněž jakým způsobem. Zařízení musí splňovat požadavky, které si státní orgán nebo jiná státní instituce stanoví pro naplnění účelu jeho pořízení.

Stanovit zákonnost zpracování osobních údajů. Údaje získané z kamerového systému nebo fotopasti musí odpovídat zákonnému zpracování podle čl. 6 Obecného nařízení, ve kterém bude nutné navázat zpracování na odst. 1 písm. f), který se týká oprávněného zájmu správce (předpokladem zpracování bude např. pořízení důkazního materiálu pro další řízení). V této souvislosti je vhodné podložit oprávněnost zpracování již zaznamenanými vniknutími do objektu, kolik takových nezákonných narušení proběhlo a zda již toto bylo řešeno v rámci přestupkového či trestního řízení. Také je potřeba odůvodnit umístění kamerového systému nebo fotopasti na konkrétním předem určeném místě (mimo jiné i z hlediska ekonomičnosti jejich využití).

Zajistit dodržení informační povinnosti. V rámci předmětného objektu bude nutné dodržet informovanost podle čl. 13 Obecného nařízení jak pro zaměstnance, tak i pro veřejnost. U zaměstnanců je nejvhodnějším řešením provést seznámení přes aktualizaci vnitřního předpisu. U veřejnosti je doporučeno u vstupu do objektu umístit upozornění, že objekt je monitorován. Návrh takového označení si správní orgán nebo instituce navrhují sami, ovšem i tento návrh musí obsahovat základní informace o správci, na kterého se může subjekt údajů obrátit s dotazem. Podoba označení vychází také z Pokynů 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky (verze 2.0, přijato dne 29. ledna 2020). Umístění takového oznámení však závisí na charakteru zaznamenávaného objektu a jeho velikosti. Rozhodně také není žádoucí, aby zaměstnanci znali konkrétní umístění takového zařízení (mimo oprávněných).

Posouzení vlivu na ochranu osobních údajů (DPIA). Potřeba zajistit posouzení vlivu na ochranu osobních údajů, jak je uvedeno v čl. 35 Obecného nařízení, vyplyne z posouzení rizik (tj. identifikace hrozeb a identifikace potenciální újmy), které je nutné rovněž zpracovat. Obecně se jedná o povinnost posuzovat dopady rizika v souvislosti se zabezpečením údajů, objemem zpracování a technologická specifika, anebo legalitou či legitimitou jejich zpracování (ačkoli v tomto případě by se přistupovalo spíše k balančnímu testu). Posouzení vlivu se neprovádí tam, kde zpracování osobních údajů vyplývá přímo ze zákona.

Některá další specifika užívání kamerového systému nebo fotopasti:

1) Musí zabírat prostor ve vlastnictví správce. Veřejné prostory jen v nezbytně nutném rozsahu. Soukromé prostory zabírat nelze. Při nastavení zorného úhlu nikdy nesmí přesáhnout zájmy a práva subjektu údajů nad zájmem správce.
2) Při zpracování technické dokumentace (zdokumentování technických a organizačních opatření) je potřeba uvést technický popis kamerového systému nebo fotopasti a jejich fungování, například typ úložiště dat (cloudové úložiště, servery správce, SD karta, odesílání dat na jiné zařízení nebo místo), jaká konkrétní data budou zpracovávána (fotografický záznam, video záznam, audio záznam), jakou formou (fotografie, video), jaká bude

sekvence ukládání a případně také výmazu, specifikovat funkce kamerového systému nebo fotopasti (odvíjí se od zakoupeného typu), kam (jakým směrem) a na co (předmětný objekt) bude zařízení směřovat, jaký prostor bude zabírat (nesmí dojít k narušení soukromého prostoru, veřejného jen v minimální míře).

3) Další povinností je uvést osoby, které budou oprávněné manipulovat s kamerovým zařízením nebo fotopastí, kontrolovat je a zabezpečovat jejich fungování, a to i z pohledu ochrany proti neoprávněnému přístupu k úložišti (fyzickému na místě nebo online na serveru). To se týká rovněž osoby, která bude zastupovat pověřenou osobu v době její nepřítomnosti. S ohledem k tomu zvážit, zda zařízení bude operovat v GSM módu či nikoli (tj. ukládání pouze na SD kartu nebo ukládání na SD kartu s možností odesílání mimo zařízení fotopasti). V rámci toho je potřeba dále konkretizovat, jakým způsobem bude případný přenos probíhat (na pracovní email, služební telefon, služební počítač, sídlo ostrahy objektu, cloudové služby, atd.) a zda bude zařízení pravidelně kontrolováno, kdy pověřený zaměstnanec vymaže zaznamenané údaje, které není účelné nadále uchovávat (tj. pro předání dalšímu orgánu), případně údaje vymaže po ověření jejich relevantnosti. Mazání dat může být nastaveno také automaticky. S tím by souviselo stanovení doby, na kterou by byla data ukládána (vždy pouze na nezbytné minimum). U kamerového systému se záznamem je doporučeno uchování záznamu nejdéle 7 dní. Tato lhůta může být v odůvodněných případech prodloužena. V případě dalšího předání by se výmaz dat řídil spisovým a skartačním řádem.
4) Nutné je také provést analýzu variant sledovaného objektu, včetně analýzy zásahu do soukromí (tj. vyhodnocení míry rizik a technický popis umístění zařízení). Má přesah do objektové bezpečnosti.
5) Je potřeba zajistit řádnou ochranu snímacích zařízení, přenosových cest a datových nosičů se záznamy, jakožto i osobních údajů tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k nim, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití (jedná se o zachování integrity, důvěrnosti a dostupnosti)

6) Umožnit použití kamerového systému nebo fotopasti pouze v nezbytné míře s přihlédnutím na ochranu práv a svobod subjektu údajů. Manipulovat se zařízením mohou pouze osoby určené správcem k manipulaci s předmětným zařízením (zaměstnanci, bezpečnostní agentura, servisní firma). V případě, že se jedná o externího poskytovatele služeb, který jakýmkoliv způsobem bude nakládat s osobními údaji správce, je nutné uzavřít příslušnou smlouvu, ve které budou konkrétně stanoveny veškeré podmínky činností a oprávnění vyplývající pro zpracovatele. Není-li zřejmý provozovatel nebo známa dokumentace kamerového systému, bude takový kamerový systém dočasně odpojen, v případě aktivního užívání vyřazen z provozu.
7) Zásadním předpokladem pro plnění povinností správce vyplývající z Obecného nařízení je také vedení příslušné dokumentace k ochraně osobních údajů v rámci jednotlivých agend, které správce zpracovává. Téma této kapitoly je zaměřeno na kamerové systémy, popř. fotopasti, a proto bude následujících několik bodů zaměřeno na dokumentaci vedenou v rámci ochrany osobních údajů při provozování záznamových zařízení, a to především těch, které umožňují videozáznam. Při vedení dokumentace je správce povinen zpracovat, plnit a vést zejména níže uvedené body (a až j).

a) Záznamy o činnostech zpracování

   Záznam o činnostech zpracování pro kamerový systém musí obsahovat tyto údaje[48]:

   i. Označení správce v podobě běžné identifikace správce (subjektu), který provádí zpracování,
   ii. Účel zpracování, kterým může být například ochrana majetku správce nebo života a zdraví osob prostřednictvím stálého kamerového systému,

[48] K provozování kamer a kamerových systémů: Role ÚOOÚ: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka [online].* Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 24.08.2022]. Dostupné z: https://www.uoou.cz/casto-kladene-otazky-ke-kameram-a-kamerovym-systemum/ds-5041/p1=4726&archiv=1

iii. Popis kategorií subjektů údajů, zejména zaměstnanci a příležitostně vstupující osoby do monitorovaného prostoru (dodavatelé, návštěvy apod.),

iv. Popis kategorií osobních údajů, kam spadá podoba a obrazové informace o chování a jednání zaznamenaných osob,

v. Příjemci osobních údajů, jimiž mohou být v odůvodněných případech orgány činné v trestním řízení, příp. jiné zainteresované subjekty pro naplnění účelu zpracování (např. pojišťovny), a informace o případném předání osobních údajů do třetích zemí

vi. Lhůta pro výmaz určující dobu uchování záznamů (obvykle ne déle než 7 dní), přičemž záznam zachyceného incidentu je uchován po dobu nezbytnou pro projednání případu a pro právní ochranu,

vii. Technická a organizační bezpečnostní opatření, jako jsou bezpečnostní kryt, řízený přístup k datům, školení oprávněných osob nebo vedení záznamů o předání nahrávek oprávněným orgánům a osobám.

b) Informační povinnost vůči subjektu údajů

Musí obsahovat jasné označení a informaci o monitorování objektu, identifikační údaje správce, kontakt na správce, příp. odkaz na webovou stránku, kde jsou poskytnuty další informace ke zpracování os. údajů.

c) Zdokumentování technických a organizačních opatření k zajištění ochrany osobních údajů při provozu zařízení

Jedná se o komplexnější materiál popisující specifikace zpracování osobních údajů, charakteristiku kamerového systému nebo jiného záznamového zařízení, opatření k ochraně osobních údajů (technická a organizační), právní úpravu a kontrolní snímky ze zařízení, přístup k záznamům nebo jejich přesun či poskytování dalším osobám

d) Posouzení vlivu na ochranu osobních údajů

Postup je v zásadě takový, že pokud nevyplývá zpracování osobních údajů přímo ze zákona, a zároveň je zjištěno vysoké riziko pro práva a svobody fyzických osob, provede se posouzení vlivu.

e) Stanovení účelu, prostředků a způsobu zpracování

Vztahuje se zejména k legalitě a legitimitě zpracování osobních údajů

f) Provést analýzu variant sledovaného objektu

   Při této analýze se posuzují například varianty rozmístění technického zařízení na objektu nebo v jeho vnitřních prostorách, včetně analýzy zásahů do soukromí a výběr nejvhodnější varianty, včetně zjištění zorného pole nebo monitorování lidí

g) Provést posouzení rizik

   Při této analýze se posuzují hrozby jako neoprávněný nebo nahodilý přístup k osobním údajům, neoprávněná změna, zničení nebo ztráta osobních údajů nebo jejich nepovolený přenos. Míra rizika je pak hodnocena na základě možnosti uskutečnění rizika a v závislosti na stávajících realizovaných opatření. Součástí pak může být například mapa rizik, která vyhodnocuje míru rizika pro subjekty údajů plynoucí ze zpracování osobních údajů nebo popisná tabulka s hodnocením hrozeb.

h) Mít k dispozici projektovou dokumentaci nebo technický popis zařízení

   Chybějící projektová dokumentace má velký vliv na další kroky, které jsou v rámci kamerového systému podniknuty, a to jak z pohledu ochrany osobních údajů, tak objektové bezpečnosti; důsledkem může být vyřazení kamerového systému z provozu, popř. je-li nutný jeho provoz složité zjišťování typů kamer a jiných součástí kamerového systému

i) Mít v držení smluvní dokumentaci

   Týká se školení externích zaměstnanců, smluv o mlčenlivosti, případně zajištění komplexního plnění podmínek dle čl. 28 Obecného nařízení, zejm. odst. 3, je-li takto kamerový systém řešen v objektu správce.

j) Mít k dispozici kopie hlášení o poskytnutí záznamu ze zařízení

   Zdokumentovaná součinnost s Policií ČR nebo jinými správními orgány

Do jisté míry je specifický kamerový systém bez záznamu, ke kterému je nutné splnit především informační povinnost vůči subjektu údajů. Závěrem je možné ještě uvést několik vzorových opatření, která by měla být v souvislosti s kamerovým systémem dodržována. Jedná se o: „řádné logování u záznamových zařízení; sjednocení časů u pořizovaných záznamů; plná funkčnost záznamového zařízení; odpovídající kvalita snímacích i zobrazovacích zařízení; plynulý chod při stahování záznamů; kvalitnější výstupy včetně

možnosti úprav záznamů (anonymizace osob) a s tím související nižší nároky na kapacitu úložiště; komplexní a aktuální projektová dokumentace ke kamerovému systému při opravách nebo pořízení nového kamerového systému; servisní opravy a revize ke kamerovému systému (zejména u el. obvodů a rozvaděčů); pravidelné kontroly záznamů ke zjištění odpovídající funkčnosti celého systému“. Vhodné je také zmínit skutečnost, že kamerové systémy nejsou předmětem zájmu pouze dozorového úřadu, ale rovněž také Státního úřadu inspekce práce[49], který je oprávněn na rozdíl od dozorového úřadu státním institucím udělovat v přestupkovém řízení i pokuty.

4.6 Úřad pro ochranu osobních údajů

Orgán dozoru (nebo také dozorový úřad) byl obecně zmíněn co do právního vymezení již v čl. 28 Směrnice 95/46/ES. Po příchodu Obecného nařízení je zakotven v čl. 51 až 59 tohoto nařízení. V našem právním prostředí byl zřízen ust. § 2 ZoOOÚ, a je jím Úřad pro ochranu osobních údajů (dále také jako „ÚOOÚ“). Jeho postavení, působnost, organizace a činnost byly rozvedeny v ust. § 28 až § 48a tohoto zákona. Po zrušení ZoOOÚ upravuje jeho postavení a pravomoc ZoZOÚ, což vyplývá z ust. § 2 písm. e) tohoto zákona. Jeho činnost, organizaci a jiné prvky dále rozvádí ust. § 50 až § 60. Další informace rozvádí např. recitál 117 až 123 Obecného nařízení. Zároveň má ÚOOÚ zásadní vliv na výklad a dodržování souladu Obecného nařízení a ZoZOÚ v prostředí právního řádu České republiky (současně s judikaturou soudů).

Po základním uvedení je možné představit některé úkoly. Důležité je ovšem také zmínit, že správce a zpracovatel a případný zástupce správce nebo zpracovatele spolupracují na požádání s dozorovým úřadem při plnění jeho úkolů, což vyplývá z čl. 31 Obecného nařízení. „*Základním úkolem každého dozorového úřadu je monitorování uplatňování Obecného nařízení s cílem chránit základní práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů. Na základě mechanismu jednotnosti dozorové úřady spolupracují mezi sebou tak,*

[49] Státní úřad inspekce práce. *Státní úřad inspekce práce* [online]. Copyright © [cit. 31.08.2022]. Dostupné z: https://www.suip.cz/

aby bylo Obecné nařízení z jejich strany uplatňováno, pokud možno jednotně.“[50] Za tímto účelem vykonává kontrolní činnost, při které se zaměřuje zejména na dodržování Obecného nařízení. V rámci výkonu své činnosti a pro zajištění procesu správního dozoru se řídí také zákonem č. 255/2012 Sb., o kontrole (kontrolní řád), zákonem č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, a zákonem č. 500/2004 Sb., správní řád[51]. Celkový výčet úkolů, které by měl ÚOOÚ vykonávat je uveden v čl. 57 Obecného nařízení. Současně přijímá také podněty od veřejnosti a dalších subjektů, které nahlásí porušení zabezpečení nebo jinou formu nevhodného nakládání či zpracování osobních údajů. Úřad je následně povinen se těmito podněty zabývat, prověřit jejich skutkový stav a v případě zjištění porušení zahájit procesní kroky k nápravě.

4.6.1 Konzultační činnost

ÚOOÚ je rovněž gestorem pro výklad Obecného nařízení. Za tímto účelem se na něj mohou obracet různé subjekty, jakož i státní instituce (většinou pověřenec určený státní institucí) a konzultovat své problémy v dané oblasti, například s určitým druhem zpracováním osobních údajů. Povinná předchozí konzultace s dozorovým úřadem může nastat pouze v případě, že státní instituci jako správci osobních údajů z provedeného posouzení vlivu na ochranu osobních údajů vyplyne, že by dané zpracování mělo za následek vysoké riziko pro práva a svobody subjektů údajů, pokud by nepřijala opatření k jeho zmírnění, a zároveň tato vysoká rizika nemohou být dostatečně správcem eliminována[52]. ÚOOÚ rovněž pořádá konzultační semináře pro pověřence a vhodné může být prostudování příručky „*Jak konzultovat s Úřadem*“[53].

---

[50] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 173.

[51] Dozorová a rozhodovací činnost: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 24.08.2022]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277

[52] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG), s. 127.

[53] Konzultace pro pověřence: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/konzultace-pro-poverence/ds-5558/archiv=0

4.6.2 Dozorová činnost

Při dozorové činnosti se ÚOOÚ řídí pravomocemi, které jsou uvedeny v čl. 58 Obecného nařízení. Těmi jsou jednak vyšetřovací pravomoci následované pak pravomocemi nápravnými, a také povolovací a poradní pravomoci. Při vyšetřování bude postupovat podle kontrolního a správního řádu (viz kap. 4.6), přičemž projednání porušení tohoto nařízení a přestupky uvedené v ust. § 61 až § 65 ZoZOÚ budou vedeny podle zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. Zároveň ukládá opatření k odstranění zjištěných nedostatků a stanovuje lhůtu pro jejich odstranění. V této souvislosti následně uveřejňuje na svých webových stránkách informace ke své dozorové a rozhodovací činnosti[54], a také zprávy o činnosti, které ukládá čl. 59 Obecného nařízení. Při své dozorové činnosti pak kromě již zmíněného Obecného nařízení provádí dále také kontrolu souladu se ZoZOÚ, ale kromě toho rovněž věcně příslušné kontroly souladu například u zákona o některých službách informační společnosti nebo u zákona o elektronických komunikacích (obojí viz kap. 2). Při dalším zájmu je možné na webových stránkách ÚOOÚ v rubrice „Dozorová a rozhodovací činnost“ nalézt ukončené kontroly ÚOOÚ za uplynulá období, včetně projednávaných přestupků. V současné době jsou veřejné subjekty, potažmo také OVM, ušetřeny od sankcí ve formě finančního postihu. Toto vyloučení umožňuje čl. 83 odst. 7 Obecného nařízení a ukládá ust. § 61 odst. 3 a § 62 odst. 5 ZoZOÚ. Sankce a pokuty dále rozvádí také ÚOOÚ[55]. Ten může veřejnému subjektu, potažmo OVM uložit nápravné opatření nebo přistoupit k jiným opatřením uvedeným v čl. 58 odst. 2 Obecného nařízení. Při kontrole má ÚOOÚ oprávnění nahlížet do dokumentace vedené státní institucí k agendě ochrany osobních údajů, a správce mu ji musí na vyžádání poskytnout. Kontroly provádějí pověření zaměstnanci dozorového úřadu.

---

[54] Dozorová a rozhodovací činnost: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277

[55] 11. Sankce, pokuty: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 26.08.2022]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287

5 Informační a kybernetická bezpečnost

Informační a kybernetická bezpečnost jsou velmi důležitým pojmem dnešní doby, kdy s technologickým pokrokem narůstají možnosti zaznamenávání našich soukromých i pracovních údajů nebo aktivit, a často se tak můžeme dostávat do situací, kdy ztrácíme kontrolu nad tím, jaké údaje jsou o nás zpracovávány. Pro představu, že i toto téma je nedílnou součástí ochrany osobních údajů je možné uvést recitál 6 Obecného nařízení, který uvádí: *„Rychlý technologický rozvoj a globalizace s sebou přinesly nové výzvy pro oblast ochrany osobních údajů. Rozsah shromažďování a sdílení osobních údajů významně vzrostl. Technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Fyzické osoby stále častěji své osobní údaje zveřejňují, a to i v globálním měřítku. Technologie změnily ekonomiku i společenský život a měly by dále usnadňovat volný pohyb osobních údajů v rámci Unie a předávání do třetích zemí a mezinárodním organizacím a zároveň zajistit vysokou úroveň ochrany osobních údajů.“* Právě v této oblasti se velmi často prolíná či doplňuje ochrana osobních údajů s informační, a také kybernetickou bezpečností.

Zajímavé vyjádření poskytl ve svém nálezu také Ústavní soud, konkrétně v bodech 122 nálezu vedeném pod spisovou značkou Pl. ÚS 45/17. Zde zmiňuje: *„Změnu trendu směrem k posílení ochrany osobních údajů, či spíše znovunalezení ztracené rovnováhy, demonstruje mimo jiné přijetí GDPR či příprava přijetí tzv. e-privacy nařízení, upravujícího oblast soukromí a elektronických komunikací namísto dosavadní stejnojmenné směrnice. Překotný vývoj informačních technologií nelze zastavit či zbrzdit žádnou právní úpravou; dosah internetu a dalších sítí umožňujících elektronickou komunikaci se neomezují na hranice jednotlivých států, jde o globální jev, celosvětový fenomén, který vnitrostátní zákonodárci řeší různě a obtížně. Je třeba se vypořádat se skutečností, že aktivním přičiněním jednotlivců vzniká nepřeberné množství nejrůznějších dat (metadat) a riziko jejich zneužití exponenciálně narůstá – tomu je třeba prostředky ochrany osobních údajů přizpůsobit“*.

Pro bližší objasnění obou pojmů, které se vzájemně propojují, lze říci, že informační bezpečnost zahrnuje ochranu informací v jakékoli podobě, zatímco cílem kybernetické bezpečnosti je ochrana informací pouze v podobě digitální, a je tedy podmnožinou bezpečnosti informační[56]. Pokud přistoupíme k rozvedené definici, pak se kybernetická bezpečnost *„zaměřuje na ochranu počítačových systémů před neoprávněným přístupem nebo jiným poškozením. Vztahuje se tedy výhradně na ochranu dat, která mají svůj původ v digitální podobě"*[57]. Informační bezpečnost *„je o něco širší kategorie, která se snaží chránit veškerá informační aktiva, ať už v tištěné nebo digitální podobě. Lze ji chápat také jako prevenci neoprávněného přístupu nebo změn během ukládání dat či jejich přenosu z jednoho počítače na druhý. Zabývá se však také ochranou fyzických dat a informací"*[58].

Různých definic lze nalézt mnohem více, ale základní charakteristika zůstane vždy obdobná. Pod kybernetickou bezpečností je možné si dále například představit také předcházení hrozbám a zranitelnostem prvků digitální techniky a technologií, s tím související hodnocení rizik a nastavování opatření na tato rizika, dále zajištění technických a organizačních opatření či realizaci systému řízení bezpečnosti informací v organizaci. Definici také uvádí komentář k zákonu o kybernetické bezpečnosti, kde se k tomuto pojmu uvádí, že se jedná o *„souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru. Tyto prostředky mohou být různého charakteru – právní, organizační, vzdělávací, technické apod. Pro účely zákona o kybernetické bezpečnosti je však nutno termín "kybernetická bezpečnost" chápat především ve smyslu právních prostředků zajišťujících ochranu kybernetického prostoru, které jsou obsaženy v tomto zákoně"*[59].

---

[56] Information security vs. cybersecurity - CleverAndSmart Management Consulting. *CleverAndSmart Management Consulting* [online]. Copyright © 2008 [cit. 22.08.2022]. Dostupné z: https://www.cleverandsmart.cz/information-security-vs-cybersecurity/

[57] Kybernetická a informační bezpečnost. Legislativa, povinnosti, útoky. *Portál o bezpečnosti práce (BOZP) a požární ochraně (PO)* [online]. Copyright © 2013 [cit. 22.08.2022]. Dostupné z: https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost/#tab2

[58] Tamtéž.

[59] MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR), s. 62.

Smyslem uvedení předchozích informací je porozumění kontextu, že na ochranu osobních údajů působí jak informační bezpečnost, tak i bezpečnost kybernetická, které se vzájemným propojením podílejí na zajištění ochrany osobních údajů jako celku. Úkolem informační nebo kybernetické bezpečnosti není primárně řešit kybernetické bezpečnostní incidenty, ale zejména jim předcházet. Rozhodně by tak nemělo docházet k situacím, které zažilo Ředitelství silnic a dálnic České republiky[60], které bylo fakticky paralyzováno po uskutečněném kybernetickém útoku a reálně uvažovalo o zaplacení útočníkům.

Podmínky bezpečnosti dále vycházejí z mezinárodních norem ISO, pro oblast informačních technologií často označovaných jako ISO/IEC standardy. Zatímco ISO je zkratkou pro mezinárodní organizaci pro standardizaci, neboli „*International Organization for Standardization*“[61], tak IEC je zkratkou pro mezinárodní elektrotechnickou komisi, tedy „*International Electrotechnical Commission*“[62]. Také sama Evropská unie považuje informační i kybernetickou bezpečnost za důležitou oblast hodnou zvýšeného zájmu a vydává nebo chystá příslušné legislativní akty, např. The Digital Services Act[63]. Neméně důležité je pak také nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“). V oblasti ochrany osobních údajů jistě stojí za zmínku návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o

[60] NÚKIB: Kyberútok na weby ŘSD byl profesionální, zašifroval data | ČeskéNoviny.cz. *České noviny | ČeskéNoviny.cz* [online]. Copyright © Copyright 2022 ČTK [cit. 22.08.2022]. Dostupné z: https://www.ceskenoviny.cz/zpravy/nukib-kyberutok-na-weby-rsd-byl-profesionalni-zasifroval-data/2208924

[61] ISO - International Organization for Standardization. [online]. Copyright © All Rights Reserved [cit. 22.08.2022]. Dostupné z: https://www.iso.org/home.html

[62] ISO - IEC - International Electrotechnical Commission. [online]. Copyright © All Rights Reserved [cit. 22.08.2022]. Dostupné z: https://www.iso.org/organization/70.html

[63] The Digital Services Act: ensuring a safe and accountable online environment | European Commission. *European Commission | Choose your language | Choisir une langue | Wählen Sie eine Sprache* [online]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), známé také pod zkratkou „*ePrivacy*“[64].

Ve státní instituci je více než vhodné k osobním údajům přistupovat i jako k aktivu informační bezpečnosti. Přestože osobní údaje mohou být jak v listinné, tak elektronické podobě, je v současné době nanejvýš pravděpodobné, že i písemná podoba bude převedena do formátu digitálního, ať již skenováním nebo přepsáním do příslušné aplikace nebo nástroje či jiné služby. V zásadě tak bude platit, že má-li státní instituce kvalitně nastaven interní systém řízení bezpečnosti informací (známý také pod zkratkou „SŘBI“), neměla by mít problém se zajištěním správné a odpovídající ochrany osobních údajů, které jsou rovněž informacemi. Osobní údaje lze pak v rámci SŘBI považovat za aktivum informační bezpečnosti[65], a nastavit požadované nebo doporučené prvky ochrany a příslušná bezpečnostní opatření. V rámci krátkého uvedení takových opatření je vhodné nahlédnout na ust. § 5 zákona o kybernetické bezpečnosti (dále jen ZoKB). Podrobnější specifika pak uvádí prováděcí právní předpis k zákonu o kybernetické bezpečnosti, jímž je vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). SŘBI (anglicky ISMS[66] neboli Information Security Management System) je široký pojem zahrnující mnoho procesů a interních politik. Pro určitou představu je upraven v ust. § 3 vyhlášky o kybernetické bezpečnosti (dále jen VoKB). Bezpečnostní opatření následně členíme na technická a organizační. Organizační uvádí § 3 až § 16 VoKB, kdežto technická jsou uvedena v ust. § 17 až § 29 VoKB. Zpracování osobních údajů je pak upraveno v ust. § 22c ZoKB.

---

[64] Úřad k návrhu nařízení o soukromí a elektronických komunikacích: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 22.08.2022]. Dostupné z: https://www.uoou.cz/urad-k-navrhu-narizeni-o-soukromi-a-elektronickych-komunikacich/d-49300

[65] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi, s. 196.

[66] Co je ISMS | TAYLLORCOX. *Manažerské kurzy, školení na míru, certifikace | TAYLLORCOX* [online]. Copyright © AXELOS Limited 2009. Copyright [cit. 31.08.2022]. Dostupné z: https://www.tx.cz/isms/metodika

V poslední době se nedílnou součástí informační a kybernetické bezpečnosti stává také zabezpečení dat a jejich zpracování u poskytovatelů cloudových služeb. U těchto služeb dochází k různému typu zpracování dat na základě nastavení dané služby. Státní instituce může poskytovatele cloudových služeb oslovit s požadavkem, kterým může být například ukládání části dat na serverech poskytovatele, anebo i provoz aplikací a systémové infrastruktury. Pro představu se jedná o typy služeb jako IaaS[67], PaaS[68] nebo SaaS[69]. V prvním případě hovoříme o infrastruktuře jako službě, ve druhém o platformě jako službě, a ve třetím o softwaru jako službě. Právě u cloud computingu[70] se můžeme setkávat kromě pojmu osobní údaj také s pojmem „*osobně identifikovatelné informace*“, vycházející z anglické zkratky PII neboli „*Personally Identifiable Information*“, a to v návaznosti na zpracování těchto informací ve veřejných datových úložištích, často označovaných jako cloud computingové služby. Pravidly pro ochranu PII se zabývá norma ISO/IEC 27018 (viz kap. 5.1). Cloud computing je v současné době také velmi aktuálním tématem. OVM mají povinnost vycházející z ust. § 4 odst. 5 ZoKB, které jim ukládá zařadit poptávaný cloud computing (tj. informační nebo komunikační systém) do příslušné bezpečnostní úrovně (jedné ze čtyř, od nízké, střední, vysoké až po kritickou), aby následně mohly tuto službu poptávat. Momentálně figurují v této oblasti dva prováděcí právní předpisy k ZoKB, přičemž v nejbližší době se chystá třetí prováděcí právní předpis o bezpečnostních pravidlech pro OVM, které budou chtít využívat již zmíněné cloud computingové služby.

---

[67] Služby IaaS – Státní pokladna Centrum sdílených služeb, s. p.. *Státní pokladna Centrum sdílených služeb, s. p.* [online]. Copyright © Copyright SPCSS 2022 [cit. 30.08.2022]. Dostupné z: https://www.spcss.cz/sluzby/iaas/

[68] Služby PaaS – Státní pokladna Centrum sdílených služeb, s. p.. *Státní pokladna Centrum sdílených služeb, s. p.* [online]. Copyright © Copyright SPCSS 2022 [cit. 04.09.2022]. Dostupné z: https://www.spcss.cz/sluzby/paas/

[69] Služby SaaS – Státní pokladna Centrum sdílených služeb, s. p.. *Státní pokladna Centrum sdílených služeb, s. p.* [online]. Copyright © Copyright SPCSS 2022 [cit. 04.09.2022]. Dostupné z: https://www.spcss.cz/sluzby/saas/

[70] Cloud computingem se podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, rozumí „*způsob zajištění provozu informačního systému veřejné správy nebo jeho části prostřednictvím dálkového přístupu k sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem informačního systému veřejné správy*“.

5.1 ISO normy

Jak již bylo nastíněno v úvodu této kapitoly, mezinárodní standardy označované zkratkou ISO jsou důležitou součástí při aplikaci různých opatření, technik a doporučení pro zajištění adekvátní informační, potažmo kybernetické bezpečnosti, která by měla být nedílnou součástí vnitropodnikové dokumentace každé státní instituce. Tato vnitropodniková dokumentace by měla obsahovat příslušné bezpečnostní politiky, které zavedou v instituci dostatečné bezpečnostní prvky, praktiky a opatření, aby bylo co nejvíce sníženo riziko narušení důvěrnosti, integrity nebo dostupnosti informací a dat. Konkrétní návrhy na ochranu těchto informací poskytují například níže uvedené normy. Pro další informace a hlubší porozumění lze doporučit studium odborné literatury[71].

1) ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky
2) ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací
3) ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací
4) ISO/IEC 27017 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002
5) ISO/IEC 27018 Informační technologie – Bezpečnostní techniky – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII
6) ISO/IEC 29100 Informační technologie – Bezpečnostní techniky – Rámec ochrany soukromí
7) ISO/IEC 29134 Informační technologie – Bezpečnostní techniky – Pokyny pro posuzování dopadů na soukromí
8) ISO/IEC 29151 Informační technologie – Bezpečnostní techniky – Kodex zásad ochrany osobních údajů

[71] NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi, s. 195 až 215.

6 Závěr

V některých případech nástup GDPR nevedl pouze ke zlepšení stávající situace, ať již z důvodu záměrného opomíjení tohoto nařízení, finančních důvodů, neodborné aplikace nařízení v prostředí instituce nebo nevhodného výkladu jednotlivých článků, které často doplňovala a stále doplňuje judikatura soudů. Povedlo se však problematiku zpracování osobních údajů dostat do popředí zájmu, zviditelnit ji a přimět odpovědné osoby, aby přistupovaly k této oblasti s větší obezřetností. S ohledem na poměrně ledabylý přístup některých státních institucí v roli správců k ochraně osobních údajů se nabízí uvést jako obecně doporučující opatření opětovné zavedení finančních pokut pro státní instituce, což by mohlo těmto subjektům poskytnout větší zájem o pravidelnou aktualizaci dokumentace a školení zaměstnanců (interní pro všechny zaměstnance, rozšířené pro vedoucí pracovníky a externí pro vybrané odborné pracovníky), prolínání ochrany osobních údajů s informační bezpečností a dodržování relevantních ISO norem, včetně fyzické bezpečnosti a pravidel podléhajících provozu kamerového systému. Zároveň je nutné pamatovat také na smlouvy a jiné obdobné dokumenty, které je nutné zpracovávat uvážlivě a s přihlédnutím k podstatným okolnostem zpracování osobních údajů v dané instituci, právnímu řádu a Obecnému nařízení. Mělo by se předcházet tomu, aby do smluv byly bez rozmyslu kopírovány pouze informace ze smluv předešlých, jelikož podmínky plnění se mohou lišit, byť se některé pasáže mohou shodovat. Neméně důležité je zajištění informační povinnosti, a to zejména při každém novém zpracování.

Instituce musí mít také zavedeny vnitropodnikové procesy k zajištění zabezpečení ochrany osobních údajů a zajistit jejich dodržování, a to jak vedoucími pracovníky, tak zaměstnanci. Není však žádoucí při úsilí vše patřičně zdokumentovat sklouzávat do přílišné administrativní zátěže, kterou pak musí různá oddělení nebo odbory plnit, leckdy pravidelně. Smyslem zavedených opatření by měla být také jednoduchost v metodice provedení a ve schopnosti jasně a určitě vymezit potřeby vyplývající z přijaté vnitropodnikové směrnice a přidružených příloh. Každá instituce může mít dokumentaci a opatření pojata odlišně. Proto je také důležité zajistit, aby sama instituce měla nejen odborníka

v oblasti ochrany osobních údajů, ale také člověka, který má prostor a čas se dostatečně obeznámit s fungováním instituce, s dokumentací k ochraně osobních údajů a vnitropodnikovou dokumentací, a aby i tento člověk byl transparentně informován o dění v instituci, které souvisí s jeho agendou.

Pověřenec pro ochranu osobních údajů ustanovený v příslušné státní instituci by pak měl být řádně informován o procesech zpracování, které v instituci probíhají, o bezpečnostních událostech nebo incidentech souvisejících s osobními údaji a sledovat pokyny Sboru pověřenců a jejich dodržování, a v případě potřeby komunikovat s dozorovým úřadem, stejně tak jako s interním zaměstnancem v instituci pověřeným výkonem agendy ochrany osobních údajů. Doporučením je tak jednoznačně vymezit osoby, které budou mít tuto činnost jako primární, a nebudou nadmíru zatěžovány jinými agendami přesahujícími časovou náročností agendu zmíněnou. Ačkoli se pochopitelně nevylučují další činnosti, které mohou uvedené osoby provádět, ať již specialista nebo pověřenec, dopadá to nejvíce na instituci samotnou, která se vystavuje riziku, že ochrana osobních údajů nebude zajištěna v požadované kvalitě a rozsahu. Potřeba jsou rovněž pravidelné metodické dohlídky pracovníkem nebo oddělením, které má ochranu osobních údajů na starost, nejlépe ve spolupráci s pověřencem.

Doporučuje se také sledovat pravidelně stránky Úřadu pro ochranu osobních údajů, kde lze nalézt doprovodné informace k různým oblastem tohoto tématu, včetně rozhodovací činnosti jmenované instituce a stanovisek k různým reálným případům, z čehož lze jistě čerpat při zajištění vlastního souladu zabezpečení.

V rámci informační a kybernetické bezpečnosti je potřeba provázat uvedené s ochranou osobních údajů a nestavit se k těmto dvěma oblastem jako vzájemně nezávislým. K tomu je nutná spolupráce zainteresovaných osob, nejlépe na pravidelné bázi. Pro tento účel může být vhodné založit pracovní či konzultační skupinu nebo výbor, který se bude pravidelně scházet a diskutovat o aktuálních problémech, vnitropodnikové dokumentaci, nových opatřeních a systémech v instituci, včetně jejich dopadu na ochranu informací a dat, jakožto také o dopadu na osobně identifikovatelné informace, obecněji řečeno „*osobní údaje*“.

7 Seznam použité literatury

7.1 Monografie

1. BŘEŇ, Jan. *Základní charakteristika státní správy*. Praha: Institut pro veřejnou správu Praha, 2017. Skripta (Institut pro veřejnou správu). ISBN 978-80-86976-44-0.
2. FIALA, Ondřej, Jan GREPL a Ondřej LICHNOVSKÝ. *GDPR: hmotné a procesní aspekty prakticky*. V Praze: C.H. Beck, 2019. Právní praxe. ISBN 978-80-7400-762-0.
3. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
4. KLÍMA, Karel. *Ústavní právo*. 4., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. Právnické učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-261-5.
5. KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.
6. MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.
7. MOLNÁR, Zdeněk. *Pokročilé metody vědecké práce*. [Zeleneč]: Profess Consulting, 2012. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3.
8. NEZMAR, Luděk. *GDPR: praktický průvodce implementací*. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-80-271-0668-4.
9. NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. Praktický komentář. ISBN 978-80-7552-765-3.
10. VIDRNA, Jan a Zdeněk KOUDELKA. *Zaměstnanci v objektivu kamer: právní aspekty monitoringu zaměstnanců*. V Praze: C.H. Beck, 2013. Beckova edice ABC. ISBN 978-80-7400-453-7.

11. VLACHOVÁ, Barbora. *Zákon o zpracování osobních údajů: komentář*. V Praze: C.H. Beck, 2019. Beckovy komentáře. ISBN 978-80-7400-760-6.
12. ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-80-7554-152-9.
13. Kučerová, Alena a kol. *Zákon o ochraně osobních údajů: komentář*. V Praze: C.H. Beck, 2012. Beckova edice komentované zákony. ISBN 978-80-7179-226-0.

7.2 Zákonná úprava a interní akty řízení

1. Ústavní zákon č. 1/1993 Sb., *Ústava České republiky*, v posledním znění
2. Usnesení předsednictva České národní rady č. 2/1993 Sb., *o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky*, v posledním znění
3. Listina základních práv Evropské unie ze dne 7. prosince 2000, konsolidované znění.
4. Smlouva o fungování Evropské unie ze dne 13. prosince 2007, konsolidované znění
5. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*, v posledním znění
6. Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 *o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Text s významem pro EHP)*, v posledním znění
7. Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 *o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti")*, v posledním znění

8. Zákon č. 2/1969 Sb., *o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky*, v posledním znění
9. Zákon č. 40/2009 Sb., *trestní zákoník*, v posledním znění
10. Zákon č. 82/1998 Sb., *o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád)*, v posledním znění
11. Zákon č. 89/2012 Sb., *občanský zákoník*, v posledním znění
12. Zákon č. 101/2000 Sb., *o ochraně osobních údajů a o změně některých zákonů*, v posledním znění
13. Zákon č. 106/1999 Sb., *o svobodném přístupu k informacím*, v posledním znění
14. Zákon č. 111/2009 Sb., *o základních registrech*, v posledním znění
15. Zákon č. 111/2019 Sb., *kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů*, v posledním znění
16. Zákon č. 123/1998 Sb., *o právu na informace o životním prostředí*, v posledním znění
17. Zákon č. 127/2005 Sb., *o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)*, v posledním znění
18. Zákon č. 133/2000 Sb., *o evidenci obyvatel a rodných číslech a o změně některých Zákonů (zákon o evidenci obyvatel)*, v posledním znění
19. Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)*, v posledním znění
20. Zákon č. 159/2006 Sb., *o střetu zájmů*, v posledním znění
21. Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*, v posledním znění
22. Zákon č. 250/2016 Sb., *o odpovědnosti za přestupky a řízení o nich*, v posledním znění
23. Zákon č. 255/2012 Sb., *o kontrole (kontrolní řád)*, v posledním znění
24. Zákon č. 256/1992 Sb., *o ochraně osobních údajů v informačních systémech*, v posledním znění
25. Zákon č. 262/2006 Sb., *zákoník práce*, v posledním znění

26. Zákon č. 273/2008 Sb., *o Policii České republiky*, v posledním znění
27. Zákon č. 304/2013 Sb., *o veřejných rejstřících právnických a fyzických osob*, v posledním znění
28. Zákon č. 365/2000 Sb., *o informačních systémech veřejné správy a o změně některých dalších zákonů*, v posledním znění
29. Zákon č. 412/2005 Sb., *o ochraně utajovaných informací a o bezpečnostní způsobilosti*, v posledním znění
30. Zákon č. 480/2004 Sb., *o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti)*, v posledním znění
31. Zákon č. 499/2004 Sb., *o archivnictví a spisové službě a o změně některých zákonů*, v posledním znění
32. Zákon č. 500/2004 Sb., *správní řád*, v posledním znění
33. Vyhláška č. 82/2018 Sb., *o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*, v posledním znění
34. Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 *o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)*, v posledním znění
35. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 *o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) - tato směrnice byla změněna Směrnicí Evropského parlamentu a rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES, o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004, o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele*, v posledním znění

36. 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 (dále jen „Směrnice 2016/680“)*, v posledním znění
37. Nařízení Komise (EU) č. 611/2013 ze dne 24. června 2013 *o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích*, v posledním znění
38. Návrh nařízení Evropského parlamentu a Rady *o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích)*, v posledním znění
39. Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s., *o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat*, v posledním znění
40. Dodatkový protokol k Úmluvě *o ochraně osob se zřetelem na automatizované zpracování osobních dat o orgánech dozoru a toku dat přes hranice (vyhlášený pod č. 29/2005 Sb. m. s.)*, v posledním znění

7.3 Webové stránky a elektronické zdroje

1. Fáze legislativního procesu v EU - Euroskop. *Hlavní strana - Euroskop* [online]. Copyright © 2005 [cit. 20.07.2022]. Dostupné z: https://euroskop.cz/evropska-unie/rozhodovani-eu/faze-legislativniho-procesu-v-eu/
2. Slovníček pojmů - Komunitární právo - BusinessCenter.cz. *BusinessCenter.cz* [online]. Copyright © 1997 [cit. 20.07.2022]. Dostupné z: https://businesscenter.podnikatel.cz/slovnicek/komunitarni-pravo/
3. Usnesení Ústavního soudu ze dne 25. 11. 1993 sp. zn. II. ÚS 75/93. NALUS - databáze rozhodnutí Ústavního soudu. *Charekteristika veřejné moci*

[online]. [cit. 22.07.2022]. Dostupné z: http://nalus.usoud.cz/Search/GetText.aspx?sz=2-75-93

4. Orgány veřejné moci v ČR | Ústav státu a práva Akademie věd České republiky. *Ústav státu a práva Akademie věd České republiky* [online]. Copyright © 2022 ÚSP [cit. 22.07.2022]. Dostupné z: https://www.ilaw.cas.cz/vyzkum/ceske-pravo-informace-a-odkazy/organy-verejne-moci-v-cr.html
5. K vymezení a aplikaci pojmu „orgán veřejné moci“ podle zákona o základních registrech - Ministerstvo vnitra České republiky. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2022 Ministerstvo vnitra České republiky, všechna práva vyhrazena [cit. 22.07.2022]. Dostupné z: https://www.mvcr.cz/clanek/k-vymezeni-a-aplikaci-pojmu-organ-verejne-moci-podle-zakona-o-zakladnich-registrech.aspx
6. Adresář úřadů - statnisprava.cz. *statnisprava.cz [online].* Copyright © Copyright 2000 [cit. 22.07.2022]. Dostupné z: https://www.statnisprava.cz/rstsp/ciselniky.nsf/druhy_uradu
7. Informace k platům a odměnám | MPO. *Ministerstvo průmyslu a obchodu* [online]. Copyright © Copyright 2005 [cit. 06.08.2022]. Dostupné z: https://www.mpo.cz/cz/rozcestnik/ministerstvo/aplikace-zakona-c-106-1999-sb/informace-zverejnovane-podle-paragrafu-5-odstavec-3-zakona/informace-k-platum-a-odmenam--266205/
8. WHO Coronavirus (COVID-19) Dashboard | WHO Coronavirus (COVID-19) Dashboard With Vaccination Data. *WHO Coronavirus (COVID-19) Dashboard | WHO Coronavirus (COVID-19) Dashboard With Vaccination Data* [online]. [cit. 25.07.2022]. Dostupné z: https://covid19.who.int/
9. Když se řekne svazek obcí | epravo.cz. *EPRAVO.CZ – Váš průvodce právem - Sbírka zákonů, judikatura, právo* [online]. Copyright © EPRAVO.CZ [cit. 23.08.2022]. Dostupné z: https://www.epravo.cz/top/clanky/kdyz-se-rekne-svazek-obci-108643.html
10. Formulář na dávky už neposílá adresy do zahraničí, ministerstvo práce ho upravilo | iROZHLAS - spolehlivé zprávy. *iROZHLAS - spolehlivé a rychlé zprávy* [online]. Copyright © 1997 [cit. 22.08.2022]. Dostupné

z: https://www.irozhlas.cz/zpravy-domov/mpsv-davky-formular-data-gdpr_2208191910_cib

11. Povinnosti správců: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 26.08.2022]. Dostupné z: https://www.uoou.cz/povinnosti-spravcu/ds-5856/p1=5856
12. Bulletin advokacie, odborný právnický portál | Analýza praktických dopadů rozhodnutí Soudního dvora EU ve věci Google Spain. *Bulletin advokacie, odborný právnický portál | Domů* [online]. Copyright © [cit. 17.08.2022]. Dostupné z: http://www.bulletin-advokacie.cz/analyza-praktickych-dopadu-rozhodnuti-soudniho-dvora-eu-ve-veci-google-spain
13. Profilování a automatizované rozhodování | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. [cit. 17.08.2022]. Dostupné z: https://www.gdpr.cz/blog/profilovani/
14. 4. Zásady a právní důvody zpracování: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 29.08.2022]. Dostupné z: https://www.uoou.cz/4-zasady-a-pravni-d-vody-zpracovani/d-27271
15. Zásady zpracování osobních údajů - Ochrana osobních údajů. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2022 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 29.08.2022]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/zasady-zpracovani-osobnich-udaju.aspx
16. Pověřenec pro ochranu osobních údajů - Ochrana osobních údajů. *Úvodní strana - Ministerstvo vnitra České republiky* [online]. Copyright © 2022 Ministerstvo vnitra České republiky. Všechna práva vyhrazena. [cit. 07.08.2022]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/poverenec-pro-ochranu-osobnich-udaju-poverenec-pro-ochranu-osobnich-udaju.aspx
17. Pověřenec pro ochranu osobních údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 07.08.2022]. Dostupné z:

https://www.uoou.cz/poverenec%2Dpro%2Dochranu%2Dosobnich%2Dudaju/ds-5550/p1=5550

18. Kdo jsme | European Data Protection Board [online]. [cit. 06.08.2022]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_cs
19. Pokyny evropského Sboru (EDPB): Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 06.08.2022]. Dostupné z: https://www.uoou.cz/pokyny%2Devropskeho%2Dsboru%2Dedpb/ds-4728/p1=4728
20. Ohlašování případů porušení zabezpečení: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 30.08.2022]. Dostupné z: https://www.uoou.cz/ohlasovani-pripadu-porusenizabezpeceni/d-30181
21. Anonymizace a pseudonymizace jsou dvě rozdílná slova | GDPR.cz. *GDPR | Obecné nařízení o ochraně osobních údajů — prakticky* [online]. [cit. 06.08.2022]. Dostupné z: https://www.gdpr.cz/blog/anonymizace-a-pseudonymizace-jsou-dve-rozdilna-slova/
22. Základní příručka k ochraně údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/zakladni-prirucka/ds-4744/p1=4744
23. Posouzení vlivu na ochranu osobních údajů: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/posouzeni-vlivu-na-ochranu-osobnich-udaju/ds-6413/p1=6413
24. Kamerové systémy - TZB-info: *Kamerové systémy* [online]. Topinfo s.r.o., Copyright © 2001-2021 [cit. 24.8.2022]. Dostupné z: https://www.tzb-info.cz/kamerove-systemy
25. Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky | European Data Protection Board [online]. [cit. 24.08.2022]. Dostupné

z: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-thro-ugh-video_cs

26. K provozování kamer a kamerových systémů: Role ÚOOÚ: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka [online].* Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 24.08.2022]. Dostupné z: https://www.uoou.cz/casto-kladene-otazky-ke-kameram-a-kamerovym-systemum/ds-5041/p1=4726&archiv=1
27. Státní úřad inspekce práce. *Státní úřad inspekce práce* [online]. Copyright © [cit. 31.08.2022]. Dostupné z: https://www.suip.cz/
28. Dozorová a rozhodovací činnost: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 24.08.2022]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277
29. Konzultace pro pověřence: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/konzultace-pro-poverence/ds-5558/archiv=0
30. Dozorová a rozhodovací činnost: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 31.08.2022]. Dostupné z: https://www.uoou.cz/dozorova-a-rozhodovaci-cinnost/ds-1277/p1=1277
31. 11. Sankce, pokuty: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 26.08.2022]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287
32. Information security vs. cybersecurity - CleverAndSmart Management Consulting. *CleverAndSmart Management Consulting* [online]. Copyright ©

2008 [cit. 22.08.2022]. Dostupné z: https://www.cleverandsmart.cz/information-security-vs-cybersecurity/

33. Kybernetická a informační bezpečnost. Legislativa, povinnosti, útoky. *Portál o bezpečnosti práce (BOZP) a požární ochraně (PO)* [online]. Copyright © 2013 [cit. 22.08.2022]. Dostupné z: https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost/#tab2
34. NÚKIB: Kyberútok na weby ŘSD byl profesionální, zašifroval data | ČeskéNoviny.cz. *České noviny | ČeskéNoviny.cz* [online]. Copyright © Copyright 2022 ČTK [cit. 22.08.2022]. Dostupné z: https://www.ceskenoviny.cz/zpravy/nukib-kyberutok-na-weby-rsd-byl-profesionalni-zasifroval-data/2208924
35. ISO - International Organization for Standardization. [online]. Copyright © All Rights Reserved [cit. 22.08.2022]. Dostupné z: https://www.iso.org/home.html
36. ISO - IEC - International Electrotechnical Commission. [online]. Copyright © All Rights Reserved [cit. 22.08.2022]. Dostupné z: https://www.iso.org/organization/70.html
37. The Digital Services Act: ensuring a safe and accountable online environment | European Commission. *European Commission | Choose your language | Choisir une langue | Wählen Sie eine Sprache* [online]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en
38. Úřad k návrhu nařízení o soukromí a elektronických komunikacích: Úřad pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: Titulní stránka* [online]. Copyright © 2013 Úřad pro ochranu osobních údajů. Všechna práva vyhrazena. [cit. 22.08.2022]. Dostupné z: https://www.uoou.cz/urad-k-navrhu-narizeni-o-soukromi-a-elektronickych-komunikacich/d-49300
39. Co je ISMS | TAYLLORCOX. *Manažerské kurzy, školení na míru, certifikace | TAYLLORCOX* [online]. Copyright © AXELOS Limited 2009. Copyright [cit. 31.08.2022]. Dostupné z: https://www.tx.cz/isms/metodika

40. Služby IaaS – Státní pokladna Centrum sdílených služeb, s. p.. *Státní pokladna Centrum sdílených služeb, s. p.* [online]. Copyright © Copyright SPCSS 2022 [cit. 30.08.2022]. Dostupné z: https://www.spcss.cz/sluzby/iaas/
41. Služby PaaS – Státní pokladna Centrum sdílených služeb, s. p.. *Státní pokladna Centrum sdílených služeb, s. p.* [online]. Copyright © Copyright SPCSS 2022 [cit. 30.08.2022]. Dostupné z: https://www.spcss.cz/sluzby/paas/
42. Služby SaaS – Státní pokladna Centrum sdílených služeb, s. p.. *Státní pokladna Centrum sdílených služeb, s. p.* [online]. Copyright © Copyright SPCSS 2022 [cit. 30.08.2022]. Dostupné z: https://www.spcss.cz/sluzby/saas/
43. ISO - ISO/IEC 27001 — Information security management. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/isoiec-27001-information-security.html
44. ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/54533.html
45. ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/75281.html
46. ISO - ISO/IEC 27017:2015 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/43757.html
47. ISO - ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/76559.html

48. ISO - ISO/IEC 29100:2011 - Information technology — Security techniques — Privacy framework. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/45123.html
49. ISO - ISO/IEC 29134:2017 - Information technology — Security techniques — Guidelines for privacy impact assessment. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/62289.html
50. ISO - ISO/IEC 29151:2017 - Information technology — Security techniques — Code of practice for personally identifiable information protection. [online]. Copyright © All Rights Reserved [cit. 30.08.2022]. Dostupné z: https://www.iso.org/standard/62726.html