VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

DOPADY OBECNÉHO NAŘÍZENÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ (GDPR) NA OBLAST KAMEROVÝCH SYSTÉMŮ

Autor práce: Radoslav Kliner, DiS.

Studijní obor: Bezpečnostně právní činnost ve veřejné správě

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2020

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú.
Žižkova 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Radoslav Kliner

Studijní program: Bezpečnostně právní činnost
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Dopady Obecného nařízení o ochraně osobních údajů (GDPR) na oblast kamerových systémů

Název bakalářské práce v anglickém jazyce: Impact of the General Data Protection Regulation (GDPR) on CCTV

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul): RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce: říjen 2019

CÍL BAKALÁŘSKÉ PRÁCE:
Cílem bakalářské práce je analýza legislativního rámce, ve kterém se nachází oblast kamerových systémů. Práce vysvětlí, na jakých základech stojí GDPR a jak GDPR v praxi změnilo zavádění a fungování kamerových systémů.

Student: Radoslav Kliner, DiS.	25.10.2019 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	25.10.19 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11.11.19 *datum*	 *podpis*
Prorektorka pro studium a vnitřní záležitosti: RNDr. Růžena Ferebauerová	12.11.19 *datum*	 *podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	13.11.2019 *datum*	 *podpis*

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce – v elektronické podobě ve veřejně přístupné části infodisku VŠERS a v tištěné podobě knihovnou VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucího a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

…….

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové, za odborné vedení práce, věcné připomínky, dobré rady, trpělivost a vstřícnost při konzultacích a vypracovávání bakalářské práce. Zejména pak své rodině a partnerce, kteří mne při studiu podporovali.

ABSTRAKT

KLINER, R., DiS., *Dopady Obecného nařízení o ochraně osobních údajů (GDPR) na oblast kamerových systémů: Bakalářská práce*. České Budějovice: Vysoká škola evropských a regionálních studií, 2020. 46 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: Obecné nařízení o ochraně osobních údajů, GDPR, Úřad pro ochranu osobních údajů, souhlas se zpracováním osobních údajů, kamerové systémy.

Pro svoji bakalářskou práci jsem si zvolil téma „Dopady Obecného nařízení o ochraně osobních údajů (GDPR) na oblast kamerových systémů“, neboť GDPR je v současnosti velice diskutované téma a oblast kamerových systémů výrazně ovlivnilo. V práci budou definovány základní pojmy a principy, na nichž je GDPR založeno a bude vysvětleno, jak GDPR ovlivnilo provozování kamerových systémů. Jako metodu práce jsem si určil analýzu. V práci budu vycházet z Obecného nařízení o ochraně osobních údajů, tištěných publikací o GDPR a konkrétních případech ze soukromých i státních institucí.

ABSTRACT

KLINER, R., DiS., *Impact of the General Data Protection Regulation (GDPR) on CCTV: Bachelor thesis*. České Budějovice: The College of European and Regional Studies, 2020. 46 p. Thesis supervisor: RNDr. Růžena Ferebauerová.

Keywords: General Data Protection Regulation, GDPR, the office for personal data protection, consent to processing of personal data, camera systems.

For my bachelor thesis I have chosen topic „*Impact of the General Data Protection Regulation (GDPR) on CCTV".* GDPR is highly debate theme today and field of camera systems (CCTV) significantly influenced. In my thesis are defined basic terms and principles of GDPR and explained how GDPR influenced administration of CCTV.

As method of my thesis I have chosen analysis. As a source I have used General Data Protection Regulation itself, printed expert publication and specific examples from private and state institution.

Obsah

Úvod

GDPR je téměř zaříkávadlo dnešní doby, slyšíme o něm všude kolem sebe, je to strašák moha firem a zároveň ochrana pro běžné lidi. Ale co to vlastně GDPR je? Kde se vzalo? Jak ovlivňuje životy lidí a fungování společností? Kdo to vše hlídá? Jak to funguje v praxi? Na tyto a další otázky se bude autor snažit v práci odpovědět.

Každého člověka od narození doprovází informace, které jsou pro něj specifické, jedinečné a které jej identifikují. Jedná se například o informace udávající datum a místo narození, jméno, příjmení, pohlaví, národnost, náboženské vyznání, zdravotní stav. Některé z těchto údajů můžou být pro jedince natolik intimní, že jejich zneužití může vést k jeho diskriminaci. Je zřejmá křehkost až zranitelnost údajů týkajících se jednotlivce, proto je zvláště v dnešní době důležité klást důraz na ochranu osobních údajů.

Jedním z důvodů pro přijetí nového nařízení byla zjištění, že tajné služby některých států mimo evropský prostor v minulosti hojně shromažďovaly údaje o občanech EU. S ohledem na rozdíly vnímání osobní svobody a odpovědnosti jednotlivce mezi Evropou a jinými státy tak bylo nutné stanovit jasná pravidla ochrany našich práv.

Evropská legislativa, kterou se doposud řídily zákony na ochranu osobních údajů, je zastaralá. V roce 1995, kdy začala platit současná směrnice na ochranu osobních údajů, neexistovaly sociální sítě, cloudová úložiště ani řada dalších technologií. Ve věku, kdy společnosti jako Facebook a Google sdílejí osobní údaje držitelů účtů výměnou za přístup a funkce stránek, se GDPR snaží vrátit zpět uživateli kontrolu nad situací. Nařízení je navrženo k ochraně dat zákazníků v novém digitálním prostředí.

Nařízení s sebou přinese rovnocennou vymahatelnost práva v celé EU, stejné sankce a mnohem těsnější spolupráci dozorových orgánů. Dopadne totiž skutečně na každého, kdo s osobními údaji při svém podnikání či působení pracuje. Občané EU tak opět získají kontrolu nad svými osobními údaji.

GDPR zavádí celou řadu nových pravidel. Jejich platnost a dodržování bude muset každý správce i zpracovatel osobních údajů prokazatelně doložit po celou dobu zpracování. Přibude mu tím velká administrativní zátěž, bude muset například dokumentovat, že zpracovává pouze ta data, která jsou ke konkrétnímu účelu nezbytná. GDPR také nabídne větší moc občanům při udělování povolení, pokud jde o to, co mohou společnosti dělat s jejich soukromými údaji, GDPR bylo navrženo tak, aby chránilo spotřebitele.

1 Cíle a metodika bakalářské práce

Autor si pro svoji bakalářskou práci zvolil téma „Dopady Obecného nařízení o ochraně osobních údajů (GDPR) na oblast kamerových systémů.“ Cílem práce je přiblížit problematiku ochrany osobních údajů, definovat základní pojmy a principy, na nichž je založena. GDPR se týká všech podniků a organizací, které v rámci své činnosti zpracovávají osobní údaje. Nařízení tedy dopadá na jakéhokoli podnikatele, který má alespoň jednoho zaměstnance či má mezi svými klienty fyzické podnikající osoby. Práce chce na základě implementace a fungování kamerových systémů představit, jak GDPR funguje v praxi. Autor v práci používá metodu analýzy, kdy jednotlivé části zkoumaného jevu, tedy GDPR, nejprve rozdělí na jednotlivé části a detailněji rozebírá jeho základní pojmy.

Druhá kapitola je věnována základním pojmům ochrany osobních údajů a načrtnutí jeho historického vývoje, obecní právní úpravě, souhlasu se zpracováním osobních údajů a fungováním Úřadu pro ochranu osobních údajů. Klíčovou částí práce je třetí kapitola, ve které se autor zabývá teorií implementace a fungováním kamerových systémů v praxi, představuje konkrétní případy fungování kamerových systémů – kamerové systémy ve školách, ve firmách, bytových domech, městské kamerové systémy a v poslední kapitole na příkladu města Třeboň představuje fungování městských kamerových systémů v praxi.

Osobními údaji jsou podle GDPR jakákoliv data, která lze použít pro identifikaci konkrétní fyzické osoby, tedy například jméno, věk, datum narození, pohlaví, fotografie, telefonní číslo, e-mailová adresa, může se ale jednat o IP adresu nebo cookie. GDPR také rozlišuje citlivé osobní údaje jako například etnickou či politickou příslušnost, vyznání, informace z rejstříku trestů, zdravotní dokumentaci, genetické a biometrické údaje. Silnější pravidla ochrany údajů od května 2018 znamenají, že občané získávají větší kontrolu nad svými údaji a podniky mají prospěch z rovných podmínek. Jeden soubor pravidel pro všechny společnosti působící v EU, ať sídlí kdekoliv. Nařízení nově zavádí princip tzv. zodpovědnosti, který spočívá v povinnosti správců a zpracovatelů údajů bez ohledu na jejich velikost nebo počet zaměstnanců zavést technická, organizační a procesní opatření za účelem prokázání souladu s principy GDPR.

2 Obecné nařízení o ochraně osobních údajů

Informace, data, údaje, to vše patří ke znakům dnešní společnosti. V posledních letech zažíváme velký rozvoj informačních technologií, které nám přinášejí příležitosti jako je komunikace na dálku, rychlejší a snazší obchodování a spoustu dalších možností, ale zároveň s těmito technologiemi přichází rizika, jako je snadné monitorování soukromí a jeho narušování. Zájem různých institucí, firem a lidí o naše osobní údaje raketově roste, a proto je zapotřebí si je chránit a mít možnost sami rozhodnout o tom, komu je svěříme a komu zpřístupníme informace, které se týkají naší osoby a také mít právo bránit se šíření takových informací bez našeho souhlasu.

GDPR dává lidem mnohem větší práva a stanovuje přísnější požadavky na zpracovávání osobních údajů pro firmy a instituce. Právo na soukromí řadíme mezi osobnostní práva, jež jsou chráněna občanským právem. Jedná se o právo jednotlivce rozhodnout se podle vlastního uvážení, zda a v jakém rozsahu mají být informace z jeho soukromí zpřístupněny ostatním. Soukromí je určitá intimní sféra života, do níž nikdo nesmí zasahovat bez svolení dotčené osoby, anebo pokud je k tomu dáno zákonné oprávnění.

Pokud tedy chceme nebo v rámci své profese musíme nakládat s osobními údaji, vždy bychom si měli nejprve uvědomit, proč údaje o nějakých lidech potřebujeme nebo chceme získávat, a z toho je pak třeba vyjít při požadavku na poskytnutí údajů, abychom zbytečně nezaznamenávali informace, které nepotřebujeme. Rozsah získávaných údajů by tak měl být jen minimální. A zároveň je také třeba dbát na to, aby zaznamenané údaje nebyly využívány v rozporu s původním cílem. Například na záznamu kamery je uložena spousta obrazových informací o všech osobách, které do sledovaného prostoru vstoupily. Tyto záznamy jsou po přiměřenou dobu uchovávány, aby případně bylo možné policii doložit informace o pachateli trestného činu. Nemohou být ale využívány například k nepřiměřenému kontrolování zaměstnanců na pracovišti.[1]

Další zásadou je mít uložené osobní údaje jen po tak dlouhou dobu, jak je nezbytné. Tato doba se může v různých případech hodně odlišovat. Od několika dnů záznamu kamery, kdy je zřejmé, že se v té době nic mimořádného nestalo, až po desítky let u zákonem stanoveného uchovávání některých dokumentů, například mzdových listů. Ne vždy končí doba nutná k uchovávání všech údajů ukončením nějaké činnosti, např. ukončením pracovního poměru nebo naplněním smluvního ujednání. V úvahu je třeba

[1] Úřad pro ochranu osobních údajů [online]. [cit. 3. 12. 2019]. Dostupné z: https://www.uoou.cz/gdpr%2Dobecne%2Dnarizeni/ds-3938/p1=3938

brát jak lhůty stanovené zákonem pro uchovávání některých dokumentů, tak případné promlčecí lhůty pro možnost podání soudní žaloby a v případě listinných dokumentů i lhůty skartační.[2]

Ochrana osobních údajů je v České republice zařazena mezi základní lidská práva a je tedy kromě nového Obecného nařízení o ochraně osobních údajů také chráněna Ústavou České republiky[3] a Listinou základních práv a svobod.[4] Listina základních práv a svobod je vedle Ústavy České republiky součástí ústavního pořádku České republiky. Článek 10 Listiny základních práv a svobod stanovuje právo každého na ochranu před neoprávněným zasahováním do soukromého i osobního života a právo na ochranu před neoprávněným shromažďováním, zveřejňováním či jiným zneužíváním údajů o své osobě. Ochrana osobních údajů je upravena zejména v třetím odstavci článku 10 Listiny základních práv a svobod, jež se vztahuje k problematice zpracování osobních údajů.

2.1 Historický vývoj GDPR

Potřeba ochrany osobních údajů vystoupila do popředí po 2. světové válce. Zrůdnost nacistického Německa týkající se holocaustu Židů byla u nás výrazně usnadněna tím, že v matrikách se u narozených osob uváděla náboženská příslušnost. Tyto zkušenosti se promítly do Všeobecné deklarace lidských práv, jež byla vydaná 10. prosince 1948 Organizací spojených národů. V článku 12 této Deklarace se stanoví, že nikdo nesmí být vystaven svévolnému zasahování do soukromí a ani útokům na svou čest a pověst.

Za prvního předchůdce GDPR se bere Úmluva Rady Evropy č. 108, která vstoupila v platnost 1. října 1985. Tuto úmluvu podepsalo všech 47 členů Rady Evropy s výjimkou Turecka. Následovala Evropská směrnice o ochraně osobních údajů (oficiální název je Směrnice 95/46/ ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů). Tato směrnice vstoupila v platnost 13. prosince 1995 a pojímala zpracování osobních údajů komplexně a stanovila členským zemím Evropské unie, čeho mají dosáhnout ve svých vnitrostátních řádech. Tato směrnice pomohla sjednotit právní rámec ochrany osobních údajů v Evropě, ale jednotlivé země si zavedení těchto doporučení vysvětlily po svém, a tak vznikla různá právní ustanovení

[2] Úřad pro ochranu osobních údajů [online]. [cit. 3. 12. 2019]. Dostupné z: https://www.uoou.cz/gdpr%2Dobecne%2Dnarizeni/ds-3938/p1=3938
[3] Ústavní zákon č. 1/1993 Sb., Ústava České republiky
[4] Usnesení předsednictva ČNR o vyhlášení Listiny základních práv a svobod, uveřejněné pod č.2/1993 Sb.

v jednotlivých státech Evropské unie. Jednotlivé novelizace těchto právních úprav způsobily ještě větší odlišnosti od původní Směrnice.[5]

Směrnice 95/46/ES byla následně doplněna rámcovým rozhodnutím Rady (číslo 2008/977/SVV), který upravuje ochranu osobních údajů v oblasti policejní a justiční spolupráce v trestních věcech. Tato směrnice vstoupila v platnost před více jak dvaceti lety, kdy neexistovaly sociální sítě, cloudová úložiště apod. Technologický pokrok v posledních letech přinesl řadu nových výzev týkajících se ochrany osobních údajů, a proto bylo nutné vypracovat novou legislativní úpravu.

Obecné nařízení o ochraně osobních údajů bylo přijato Evropským parlamentem a Radou EU 27. dubna 2016 a v účinnost vešlo 25. května 2018. Toto nařízení zrušilo dosavadní Směrnici 95/46/ES. Vývoj technologií se však od té doby nezastavil. Dnes můžeme říci, že i přesto, že se jedná o nejkomplexnější pravidla na ochranu dat na světě, zaostávají za technologickým pokrokem zhruba o pět let. Neřeší třeba internet věcí nebo běžnou praxi, kdy si pro výkon práce přineseme vlastní zařízení. Dá se tedy očekávat, že budou následovat další právní předpisy, které budou GDPR upřesňovat a doplňovat.[6]

Jaký je tedy rozdíl mezi Nařízením a zákonem? „*Pokud jde o stanovení práv a povinností, není mezi nařízením a zákonem rozdíl, oba dva právní předpisy přímo adresátům stanovují povinnosti a práva. Jistou zvláštností nařízení oproti zákonu je jeho Preambule, která obsahuje tzv. recitály, což jsou ustanovení předcházející vlastnímu textu nařízení a tato ustanovení jsou v některých případech výkladem či do jisté míry důvodovou zprávou k některým ustanovením vlastního textu nařízení. Je tak vhodné při práci s nařízením sledovat i jednotlivé recitály, které se např. týkají konkrétního článku či institutu nařízení.*“[7]

2.2 Obecní právní úprava GDPR

„Obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation), plným názvem nařízení Evropského parlamentu a Rady (EU) č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), představuje právní rámec ochrany osobních údajů platný na celém území Evropské unie,

[5] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 15 s. ISBN 978-80-7554-152-9
[6] QCOM [online]. [cit. 5. 12. 2019]. Dostupné z: http://www.qcom.cz/systemy-rizeni/gdpr/proc-vzniklo-gdpr/
[7] Ministerstvo vnitra ČR [online]. [cit. 7. 12. 2019]. Dostupné z: https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

který hájí práva jejích občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. GDPR přebírá všechny dosavadní zásady ochrany a zpracování údajů, na nichž unijní systém ochrany osobních údajů stojí.“[8]

Obecné nařízení představuje daleko důmyslnější a propracovanější systém ochrany osobních údajů oproti Směrnici 95/46/ES, který spočívá zejména v novém pojetí odpovědnosti správce za zajištění a dokládání souladu zpracování s Obecným nařízením a propracovanější pojetí přístupu založeného na riziku. Obecné nařízení chápe rozdílnost rizika u každého správce a podle rizika zpracování daného správce mu stanovuje méně či více povinností.[9]

Cílem obecného nařízení je přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektů údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu obecného nařízení a dozoru jednotlivými dozorovými úřady.

2.2.1 Předmět a působnost GDPR

Předmět zákonné úpravy lze rozdělit do třech základních okruhů. U první oblasti předmětu úpravy je důležité zdůraznit, že právní úprava se vztahuje na zpracování osobních údajů jen fyzických osob. Netýká se osob právnických. Pokud je osobní údaj fyzické osoby (jméno, příjmení, adresa bydliště) součástí údajů, které jsou zpracovávány jako údaje o právnických osobách, zůstává údaj vždy osobním údajem.[10] Při zpracování údajů vyplývá pro správce a zpracovatele povinnost postupovat v souladu s uvedeným zákonem.

Oblast práv a povinností je dalším okruhem předmětu zákonné úpravy. Na straně jedné jsou to práva subjektu údajů a na straně druhé povinnosti správce či zpracovatele osobních údajů. Kdokoliv, kdo nakládá s osobními údaji způsobem, který zákon vymezuje jako zpracování osobních údajů, musí konat za podmínek stanovených zákonem. Vymezení práv a povinností je rámcové a jedná se o obecnou právní úpravu. V českém právním řádu je řada zvláštních zákonů, které práva a povinnosti správce nebo zpracovatele upravují.[11]

[8] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 27 s. ISBN 978-271-0668-4
[9] ŽŮREK, J. Praktický průvodce GDPR. Olomouc: Anag, 2018. 23 s. ISBN 978-80-7554-152-9
[10] KUČEROVÁ, A.; BARTÍK, V.; PECA**,** J.; NEUWIRHTH, K.; NEJEDLÝ, J. *Zákon o ochraně osobních údajů - komentář.* 1. vyd. Praha: C.H.Beck, 2003. 34 s. ISBN: 80-7179-762-6
[11] MATOUŠOVÁ, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích.* 1. vyd. Praha: ASPI, a.s., 2004. 10s. ISBN 80-7357-037-8

Působnost lze obecně označit jako vymezení rozsahu a realizace právního předpisu a lze ji dělit na osobní, věcnou, místní a časovou.

Osobní působnost stanovuje okruh subjektů (adresátů), na které se právní předpis vztahuje. Adresáty Obecného nařízení jsou zejména správci, zpracovatelé, ale také akreditované subjekty po monitorování kodexů chování nebo subjekty pro vydávání osvědčení. Obecné nařízení těmto subjektům stanovuje práva a povinnosti, úkoly a pravomoci, jež se na adresáty vztahují. Do určité míry jsou adresáty i jednotlivé členské státy, kterým Obecné nařízení nařizuje v některých oblastech přijmout konkrétní úpravu na zákonné úrovni.[12]

Věcná působnost vymezuje, jaké vztahy právní předpis upravuje. Vztahuje se na zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci (strukturovaný soubor osobních údajů přístupných dle zvláštních kritérií) nebo do ní mají být zařazeny. Z působnosti Obecného nařízení je vyjmuto zpracování osobních údajů, které provádí fyzická osoba v rámci výlučně osobních či domácích činností. Do této činnosti lze zařadit např. vedení vlastních záznamů, korespondenci, vytváření adresářů nebo využívání sociálních sítí bez jakékoliv souvislosti s profesní nebo obchodní činností.[13]

Místní působnost vymezuje působnost právního předpisu na určité území, zejména na to, kde lze jeho aplikaci efektivně vymáhat prostřednictvím dozorových úřadů. Z geografického hlediska se Obecné nařízení aplikuje v členských státech Evropské unie. Obecné nařízení se vztahuje na zpracování osobních údajů, k němuž dochází v souvislosti s činností provozovny správce nebo zpracovatele v Evropské unii bez ohledu na to, zda zpracování probíhá v Evropské unii či mimo ni (ochrana osobních údajů cestuje s osobními údaji). Tím je zaručeno, že se správci nebo zpracovatelé nepokusí vyhnout dopadům Obecného nařízení tím, že zpracování osobních údajů záměrně provedou mimo Evropskou unii. Obecné nařízení se vztahuje i na správce, který není usazen v Evropské unii, ale na místo, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného. Jedná se o diplomatické mise nebo konzulární zastoupení členského státu.[14]

Časová působnost vymezuje dobu, po kterou je právní předpis součástí právního řádu. Rozlišujeme mezi platností a účinností právního předpisu. Platnost znamená, že právní předpis prošel stanoveným legislativním procesem a byl vyhlášen v příslušné

[12] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 36 s. ISBN 978-80-7554-152-9
[13] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 37 s. ISBN 978-80-7554-152-9
[14] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 39 s. ISBN 978-80-7554-152-9

sbírce, čímž se stává součástí právního řádu. Účinnost znamená, že právní předpis je pro adresáty závazný a může být aplikován. Obecné nařízení vstoupilo v platnost dne 24. května 2016 a do účinnosti 25. května 2018. Od tohoto data je Obecné nařízení přímo aplikovatelné na jeho adresáty a zároveň vynutitelné.[15]

2.2.2 Vymezení základních pojmů GDPR

Mezi nejdůležitější a nejvíce používané termíny v oblasti ochrany osobních údajů jsou: osobní údaj, zpracování osobních údajů, subjekt údajů, profilování, správce a zpracovatel.

Osobním údajem je každá informace o fyzické osobě, kterou lze tato osoba identifikovat. Identifikátory mohou být: jména, čísla, síťový identifikátor (př. IP adresa) nebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity konkrétní osoby. Osobními údaji nejsou pouze obecně známé identifikační údaje typu jméno, příjmení, adresa, datum narození apod., ale také např. údaje o platu či o odměnách konkrétního zaměstnance, a to nejen označeného jménem i příjmením, ale např. i jedinečným označením pozice, kterou zastává, jelikož je podle ní identifikovatelný. Osobními údaji nejsou údaje o právnických osobách (např. název, forma, základní kontaktní údaje). Pokud jde o údaje o členech statutárních orgánů či společníků, jedná se v případě fyzických osob již o osobní údaje. Osobním údajem je také personalizovaný e-mail (např. jméno.prijmeni@jmenofirmy.cz) patřící právnické osobě.[16]

Zpracováním osobních údajů se rozumí jakákoli 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. Zpracování osobních údajů ve smyslu Obecného nařízení však nelze chápat jako jakékoliv nakládání s osobním údajem, ale takové, kde se s osobními údaji nakládá za určitým účelem a činí se tak systematicky.[17] U zpracování osobních údajů není také rozhodné, zda dochází ke zpracování osobních dat automatizovaně nebo manuálně. „*Podstatnou částí definice je skutečnost, že se nemusí vždy jednat o celý soubor činností, ale může jít v některých případech jen o některé z nich,*

[15] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 40-41 s. ISBN 978-80-7554-152-9
[16] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 42-43 s. ISBN 978-80-7554-152-9
[17] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 31 s. ISBN 978-271-0668-4

dokonce se může jednat o operaci jedinou.“[18] Zpracováním se rozumí shromažďování údajů, ukládání na nosiče informací, zpřístupňování, ale též i operace jako je vyhledávání, třídění či blokování nebo likvidace dat. Typickými zpracováními jsou např. personální agenda, zákaznické systémy, evidence obyvatel, různé zákonné veřejné rejstříky obsahující osobní údaje apod. „*Zpracováním ve smyslu Obecného nařízení není např. pořízení fotografie zaměstnanců na vánočním večírku pro účely jejich následného rozeslání účastníkům či uvedení ve vnitropodnikovém časopisu nebo pro zachycení daného okamžiku a atmosféry na památku. Naopak o zpracování ve smyslu Obecného nařízení by se již jednalo, pokud by zaměstnanci byli fotografováni či by poskytovali fotografii pro účely uložení do personálního systému nebo na intranet, jelikož by byla přiřazena ke konkrétním osobám v rámci probíhajícího zpracování.“*[19]

Subjektem údajů je fyzická osoba, které se týkají osobní údaje. Subjektem údajů není právnická osoba. Typicky jde o rezidenty EU, jejichž práva Obecné nařízení chrání. Údaje vztahující se k právnické osobě tak nejsou osobními údaji. Osobní údaje mohou být pouze ve vtahu k žijící fyzické osobě, jelikož Obecné nařízení vylučuje svoji působnost na údaje o zesnulých osobách. Subjekt osobních údajů má právo přístupu k údajům a právo na jejich přenositelnost, má také právo na opravu, výmaz, právo vznášet námitky a má právo na omezení zpracování dat.[20]

Profilování je forma automatizovaného zpracování osobních údajů na základě, které dochází k vyhodnocení nebo předvídání aspektů v chování osob. Mezi formy profilování řadíme např. hodnocení pracovního výkonu osob, vyhodnocení jejich ekonomické situace pro účely nabídky vhodného finančního nebo pojistného produktu, zdravotního stavu, osobních preferencí, zájmů, místa, kde se nachází nebo pohybu. K profilování dochází i v současné době např. ve finančních službách, kdy finanční subjekty profilují např. klienta žádajícího o hypotéku, u kterého hodnotí schopnost splácet.[21] Profilování může být využito třemi různými způsoby: obecné profilování, rozhodování založené na profilování a výhradně automatizované rozhodování, včetně profilování. V prvním případě jde o situaci, kdy na základě profilu sestaveném pomocí automatizovaných procesů rozhoduje člověk. Ve druhém případě o situaci rozhoduje předepsaný algoritmus a jeho rozhodnutí je doručeno subjektu údajů bez zásahu lidského

---

[18] KUČEROVÁ, A.; BARTÍK, V.; PECA**,** J.; NEUWIRHTH, K.; NEJEDLÝ, J.*. Zákon o ochraně osobních údajů - komentář.* 1. vyd. Praha: C.H.Beck, 2003. 54 s. ISBN: 80-7179-762-6

[19] ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: Anag, 2018. 42-43 s. ISBN 978-80-7554-152-9

[20] NONNEMANN, F.; LIDINSKÝ, V.; MAŠÍN, D. *Praktická příručka GDPR pro Správce, Zpracovatele a Pověřence ochrany osobních údajů.* Praha: Nakladatelství Klika, 2018. 89 s. ISBN 978-80-88298-10-6

[21] GDPR.cz [online]. [cit. 15. 12. 2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/profilovani/

faktoru. Automatizované rozhodování může mít na subjekt údajů značný dopad. Příkladem může být přiznání nebo naopak odmítnutí zákonem garantované sociální dávky, či podrobení zvýšené úrovni bezpečnostních opatření.[22]

Správce je nejdůležitější pojem v oblasti ochrany osobních údajů. Správcem může být jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů. Správce je hlavním adresátem povinností v Obecném nařízení.[23] Správce osobních údajů je tedy každý subjekt, který určuje účel a prostředky zpracování osobních údajů. Správce provádí za jím stanoveným účelem jejich shromažďování, zpracování a uchování. Správce primárně odpovídá za zpracování osobních údajů. Základním nezbytným předpokladem je existence řádného právního důvodu zpracování osobních údajů, kterým správce musí disponovat, aby vůbec mohl osobní údaje zpracovávat. Zároveň je nutné osobní údaje dostatečně zabezpečit. Správcem může být i fyzická osoba. Správce odpovídá za dodržování zásad zpracování, za dodržování povinností upravených nařízením a za zabezpečení údajů. Významnými povinnostmi správce jsou: aplikovat záměrnou a standardní ochranu osobních údajů, jmenovat pověřence pro ochranu osobních údajů (netýká se všech správců), posuzovat vliv na ochranu osobních údajů a provádět předchozí konzultace, ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a oznamovat případy porušení zabezpečení osobních údajů subjektu osobních údajů (fyzickým osobám, jež se údaje týkají) a vést záznamy (netýká se všech správců).[24]

Zpracovatel je subjekt, kterého si správce najímá, aby pro něj prováděl zpracovatelské operace. Zpracovatel zpracovává osobní údaje pouze na základě doložených pokynů správce. „*Zpracovatel musí postupovat podle smlouvy nebo právního předpisu, které jej zavazují vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Osobní údaje musí být adekvátně zabezpečeny i u zpracovatele. Zpracovatel nesmí zapojit do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce.*“[25] Je nutné rozlišit, pro jaký účel zpracovatel osobní údaje zpracovává, neboť i zpracovatel může být

[22] GDPRsoulutions.cz [online]. [cit. 15. 12. 2019]. Dostupné z: ttps://www.gdprsolutions.cz/automaticke-zpracovani-profilovani/
[23] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 90 s. ISBN 978-80-7554-152-9
[24] GDPR.cz [online]. [cit. 6.12. 2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/
[25] UOOU [online]. [cit. 9. 12. 2019]. Dostupné z: https://www.uoou.cz/zpracovatel/d-29316/p1=3938

správcem – např. personální agentura, kdy zpracovatel zpracovává údaje pro vlastní účely. Na zpracovatele se vztahují především ustanovení o zabezpečení osobních údajů. Správce si zpracovatele může přizvat kdykoli, nepotřebuje k tomu souhlas subjektu údajů. Důvodem je, že zpracovatel je vázán pokyny správce a zpracování provádí pouze pro účely definované správcem, nikoli pro své účely. Nejčastěji správci využívají zpracovatele z důvodu, že na zpracování osobních údajů nemají dostatek personálu nebo technické prostředky. Správce může využít služby pouze takového zpracovatele, který zajišťuje dostatečné záruky použití vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky Obecného nařízení a byla zajištěna ochrana práv subjektu údajů.[26] Každé zpracování může mít jiné požadavky na kvalitu a rozsah zpracování. Správce je však primárně odpovědný za uzavření smlouvy či jiného právního aktu vymezujícího vztah mezi správcem a zpracovatelem. Účelem smlouvy je zajistit bezpečnost osobních údajů při využití zpracovatele a nastolit právně vyvážený, a pro osobní údaje bezpečný, vztah mezi správcem a zpracovatelem. Odpovědnost správce při využití zpracovatele se nikdy zcela nepřenáší a nezaniká. „*Nicméně v případě, kdy by došlo k porušení zcela na straně zpracovatele, byla by odpovědnost správce za takové porušení zpravidla vyloučena. Správce by však mohl být konfrontován s tím, že nezvolil zpracovatele bez dostatečného prověření, tj. takového, jenž by poskytl dostatečné záruky.*“[27] Pokud se zapojí do zpracování osobních údajů další zpracovatel, hovoříme o řetězení zpracovatelů. Není vyloučeno ani další větvení, ale bez vědomí a souhlasu správce není možné. Důvodem je, že správce odpovídá za zpracování a musí dbát na správný výběr zpracovatele. Zapojením dalšího zpracovatele nesmí dojít ke snížení standardu ochrany osobních údajů.

2.2.3 Práva a povinnosti při zpracování údajů GDPR

K základním stavebním pilířům ochrany osobních údajů patří povinnosti při zpracování osobních údajů. Povinnosti jsou ukládány správci a zpracovateli, jejich zaměstnancům a jiným osobám, které zpracovávají osobní data na základě smlouvy se správcem či zpracovatelem.[28] Zásady zpracování osobních údajů lze považovat za základ celé ochrany osobních údajů při jejich zpracování.

---

[26] JANEČKOVÁ, E. *GDPR Praktická příručka implementace.* Praha: Wolters Kluwer ČR, a.s., 2018. 56s. ISBN 978-80-7552-248-1.

[27] ŽŮREK, J. *Praktický průvodce GDPR.* Olomouc: Anag, 2018. 90-95 s. ISBN 978-80-7554-152-9

[28] MATOUŠOVÁ, M.; HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. vyd. Praha: ASPI, a.s., 2008. 196 s. ISBN 978-80-7357-322-5

Správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu, osobní údaje musí být shromažďovány pro jasné a legitimní účely (zásada zákonitosti), osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány (zásada omezení účelu), osobní údaje musí být přesné, uloženy ve formě umožňující identifikaci subjektu údajů jen pro nezbytnou dobu pro dané účely (zásada omezení uložení), pro které jsou zpracovány a v neposlední řadě musí být dáno technické a organizační zabezpečení osobních údajů (zásada integrity a důvěrnosti). V Obecném nařízení je stanovena odpovědnost správce za nedodržování těchto zásad, správce musí být schopen dodržování těchto zásad doložit. Jedná se o tzv. princip odpovědnosti správce.[29]

Osobní údaje může správce zpracovávat pro různé účely, ale pro každý z těch účelů potřebuje právní důvod. Zpracování osobních údajů se vždy váže k účelu, na základě kterého se určí právní důvod zpracování. Je možné i totožné osobní údaje zpracovat pro různé účely, přičemž tyto účely mohou v čase vznikat či zanikat, aniž by to představovalo povinnost osobní údaje likvidovat. Povinnost likvidace osobních údajů nastane v případě, kdy správce pozbude poslední právní důvod ke zpracování osobních údajů.[30]

Subjekt údajů má také svá práva. Oproti zákonu o osobních údajích má subjekt údajů výrazně detailněji zpracovaná práva. Jedná se především o právo na informace, na přístup k osobním údajům, tak i zcela nová práva, mezi kterými vyčnívá právo na přenositelnost. "*Ze strany správců bývá výkon práv subjektu údajů v praxi mnohdy podceňován a není mu věnována patřičná pozornost. Je nutné poznamenat, že výkon práv subjektu údajů je vysoce chráněný zájem, jehož porušení Obecné nařízení oceňuje vyšší možnou sazbou pokuty než porušení méně závažných povinností. "*[31]

Správce musí subjekt údajů při nakládání s jejich osobními údaji informovat stručným, transparentním, srozumitelným a snadno přístupným způsobem. Informace se poskytují písemně, případně elektronicky a vyloučeno není ani ústní sdělení. Časté je zveřejňování obecných informací o zpracování na internetových stránkách.[32]

[29] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 33 s. ISBN 978-271-0668-4
[30] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 33 s. ISBN 978-271-0668-4
[31] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 130 s. ISBN 978-80-7554-152-9
[32] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 131 s. ISBN 978-80-7554-152-9

2.2.4. Souhlas se zpracováním osobních údajů

"Souhlas se zpracováním osobních údajů je svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů. Jde o aktivní a dobrovolný projev vůle subjektu údajů, ke kterému nesmí být nucen."[33] Souhlas je jedním z právních důvodů, na základě kterého může správce osobní údaje zpracovávat a nastupuje tehdy, pokud zpracování nelze podřadit pod účely, pro které není nutné souhlas vyžadovat. Souhlas se vždy poskytuje k určitému účelu zpracování, který musí subjekt údajů znát. Souhlas musí být konkrétní, informovaný, jednoznačný a ničím nepodmíněný.[34]

Souhlas musí být udělen ve formě prohlášení nebo jiným jednoznačným pozitivním postupem. Získání souhlasu je nejjednodušší způsob zajištění toho, aby zpracování osobních údajů bylo zákonné. Souhlas musí být svobodný, to znamená, že správce musí zajistit, aby subjekt údajů měl právo souhlas neudělit. Svobodnou vůli osoby může podle GDPR ohrozit i tzv. nerovnovážnost vztahu se subjektem. Týká se to hlavně vztahů občanů se zaměstnavateli či orgány veřejné moci, kteří jsou zároveň správci osobních údajů. Správce v takovém postavení k subjektu by se měl vždy snažit opřít svou činnost o některý z ostatních titulů pro zpracování osobních údajů, tj. nezbytnost pro plnění smlouvy či oprávněné zájmy správce, a souhlas by měl být až tou poslední variantou, neboť v tomto případě bude vždy otázkou skutečná míra svobody při poskytnutí souhlasu. Bude-li například student veřejné školy požádán o souhlas s umístěním své fotky do školního časopisu, přičemž případné odmítnutí pro něho nebude mít sebemenší negativní následky, nebude „svoboda" rozhodování nikterak narušena.[35]

Novinkou v oblasti souhlasu se zpracováním osobních údajů je oproti zákonu o ochraně osobních údajů přímé stanovení podmínek pro vyjádření souhlasu. Tyto podmínky výrazně posilují postavení subjektu údajů. Subjekty údajů byly často nuceny dávat souhlas se zpracováním osobních údajů, aby se dostaly ke službě, kterou primárně požadovaly. Nově už tato praxe nebude možná a subjekt údajů bude mít skutečně svobodnou volbu, zda souhlas udělí či nikoliv.[36]

Souhlas musí být také konkrétní, což znamená, že v souhlasu musí být specifikace přesného účelu zpracování. Subjekt údajů nemůže souhlasit s něčím, o čem není

[33] UOOU [online]. [cit. 26. 12. 2019]. Dostupné z: https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=1881
[34] GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/gdpr/heslo/souhlas-se-zpracovanim-osobnich-udaju/
[35] GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/blog/souhlas/
[36] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 72 s. ISBN 978-80-7554-152-9

dostatečně informován. Je povinností správce údajů zajistit, aby byly informace jasné a srozumitelné. Žádost o souhlas musí být natolik konkrétní, aby v ní každý rozpoznal přesný účel zpracování, a v případě, že účelů má být více, musí být uveden každý zvlášť a o každém musí mít osoba možnost se rozhodnout samostatně. Pokud správce sloučí několik účelů zpracování a nepokusí se získat souhlas odděleně pro každý z účelů, nelze mluvit o svobodě volby. Subjekt údajů nemůže souhlasit s něčím, o čem není dostatečně informován. Souhlas se zpracováním údajů nelze použít pro jiný účel zpracování osobních údajů, než pro který byl udělen. Kvůli transparentnosti musejí být veškeré tyto informace týkající se žádosti o souhlas viditelně odděleny od jakýchkoliv nesouvisejících sdělení.[37]

Souhlas musí být také jednoznačný. „Ve většině případů správce nabídne subjektu údajů souhlas v písemné formě a vše, co je třeba k udělení souhlasu, je potvrzení subjektu údajů podpisem, že rozumí, souhlasí a schvaluje udělení souhlasu. Pro správce z toho plyne, že souhlas, jak je napsán, nesmí být zavádějící a musí v něm být jasně uvedeno, že subjekt údajů skutečně souhlas ke zpracování udělil. Souhlas musí být udělen formou prohlášení nebo jasným souhlasným jednáním, třeba zakliknutím odpovídajícího pole na webovém formuláři.“[38]

Kromě písemného souhlasu (vzor souhlasu je přílohou číslo 1 této práce) lze udělit souhlas tzv. zjevným potvrzením. Jedná se o aktivní činnost, kterou subjekt údajů vykoná, než aby byl nečinný, tedy že „mlčení je souhlas“, zde neplatí. Příkladem udělení souhlasu zjevným potvrzením je například popup okno na webové stránce, kde se na zaškrtávacím políčku zaškrtává udělení souhlasu se zpracováním osobních údajů. Naopak stejné zaškrtávací políčko, které předpokládá udělení souhlasu, když jedinec nic neudělá, nelze chápat jako aktivní udělení souhlasu. Také nelze použít přednastavené pole s již nastaveným zaškrtnutým textem „Pro neudělení souhlasu zrušte zaškrtnutí“. Takovýto postup je zcela proti duchu nařízení a nelze jej akceptovat.[39]

Výslovný souhlas je přísnější kategorií obyčejného souhlasu. Správce jej musí získat, pokud bude zpracovávat citlivé údaje, například o rasovém či etnickém původu, náboženském vyznání, členství v odborech, či zpracovávat genetické údaje, biometrická data nebo údaje o zdravotním stavu, sexuální orientaci či pokud by měly být osobní údaje využity pro automatizovaná rozhodování. Je velmi důležité, aby z uděleného souhlasu

[37] GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/blog/souhlas/
[38] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 130-131 s. ISBN 978-271-0668-4
[39] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 131 s. ISBN 978-271-0668-4

vyplývalo, že ho učinila osoba, která se zpracováním daných údajů výslovně souhlasí. Příkladem může být vlastnoruční či elektronický podpis, potvrzovací e-mail propojený se SMS zprávou nebo naskenování vlastnoručně podepsaného formuláře on-line.[40]

Každý správce musí být schopen doložit souhlas subjektu se zpracováním jeho osobních údajů, a to kdykoliv po dobu, po kterou zpracování probíhá. Proto není vhodné zpracovávání nadměrného množství dat a jejich uchovávání po dobu delší, než je nezbytně nutné. Správce by měl zaznamenat a uchovávat informace, kým byl souhlas poskytnut, jakým způsobem a v jaké podobě, jaké informace byly subjektu přístupné v žádosti o souhlas a také kdy byl souhlas udělen. V případě telefonického udělení souhlasu je třeba uchovávat nahrávku této části hovoru, ve které je osoba seznámena s informacemi, na jejichž základě poskytne svůj souhlas ke konkrétním účelům zpracování osobních údajů. Správce by neměl zapomínat ani na povinnost souhlas po čase obnovit, jelikož jednou udělený souhlas nelze chápat jako časově neohraničený. Nařízení sice žádný přesný časový požadavek pro jeho obnovu neobsahuje, ale vždy by se tak mělo stát při jakékoliv změně v procesu zpracování, o které by měl být subjekt informován.[41]

Udělení souhlasu není jediný způsob, jak zajistit možnost zpracování osobních dat. Nejčastější situací, kdy není potřeba souhlasu se zpracováním osobních údajů, je zpracování nezbytné k plnění uzavřené smlouvy, jejímž účastníkem je subjekt údajů. Další taková situace nastává u uzavření smlouvy na žádost subjektu údajů. V takovém případě se jedná o shromažďování základních údajů o subjektu údajů před vytvořením smlouvy nebo zpracování osobních údajů za účelem splnění požadavků smlouvy. Dalším případem zpracování osobních dat bez udělení souhlasu je případ, kdy je zpracování nezbytné, aby správce splnil svou zákonnou povinnost. Jedná se například o banky, které zpracovávají informace o svých klientech, aby mohly splnit zákonné povinnosti, které jim ukládá legislativa proti praní špinavých peněz apod. Správce však nesmí zpracovávat více dat, než je nezbytně nutné pro tento účel. Dalším případem je situace, kdy je zpracování dat nezbytné pro úkol vykonávaný ve veřejném zájmu nebo při výkonu veřejné moci svěřené správci. Týká se to především policie, celní správy, finanční správy apod. Pokud je zpracování nezbytné k ochraně něčích životních zájmů (bezpečností nebo zdravotní důvody, hospodářské zájmy), tak také není vyžadován souhlas se zpracováním osobních údajů.[42]

[40] GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/blog/souhlas/
[41] GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/blog/souhlas/
[42] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 131-132 s. ISBN 978-271-0668-4

Subjekt údajů může svolení se zpracováním osobních údajů jak dát, tak i kdykoli odvolat. Momentem odvolání je správce povinen zastavit zpracovávání osobních údajů. Udělení souhlasu je dáno na stejnou úroveň jako jeho odvolání. Odnětí souhlasu musí být stejně snadné jako jeho udělení.[43] V případě, kdy je souhlas poskytnut jednoduchým kliknutím myší či zmáčknutím klávesy, doporučuje se tuto formu zachovat i pro jeho odvolání. Vyžadovat pro odvolání v těchto případech například telefonní hovor není možné. Odvolání nesmí být jakkoliv zpoplatněno. Pokud je souhlas získán přes sekci pro uživatele nebo webový formulář, pak musí být jeho odvolání umožněno skrze stejnou členskou sekci a uživatele nelze odkázat na zcela jinou část webu. V případě, kdy je souhlas odvolán a neexistuje zde jiný titul pro zpracovávání údajů subjektu, je správce povinen tato data vymazat či anonymizovat. Často se však může stát, že určitá data budou kryta titulem jejich nezbytnosti pro plnění smlouvy, a proto se těchto údajů odvolání souhlasu nedotkne v plné míře, nedojde-li například i k odstoupení od smlouvy. O „přechodu“ na tento alternativní titul pro zpracovávání však musí být subjekt vždy informován.[44]

2.2.5 Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů (ÚOOÚ, dále jen “Úřad“) je nezávislý orgán, který provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů, vede registr povolených zpracování osobních údajů, přijímá podněty a stížnosti občanů na porušení zákona, poskytuje konzultace v oblasti ochrany osobních údajů. Činnost Úřadu je vymezena zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a některými dalšími zákony. Smyslem zákona o ochraně osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným zasahováním do jeho soukromého a osobního života a neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů**.** V současné společnosti je vlivem rozvoje informačních technologií toto právo stále více narušováno.[45]

Úřad byl zřízen 1. června 2000 jako nezávislý správní orgán v oblasti ochrany osobních údajů. Úřad se postupně ujal dozoru nad dodržováním povinností stanovených zákonem při zpracování osobních údajů, vedení registru povolených zpracování osobních údajů, přijímání podnětů a stížností na porušení zákona, poskytování konzultací,

[43] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 131 s. ISBN 978-271-0668-4
[44] GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/blog/souhlas/
[45] UOOU [online]. [cit. 26. 12. 2019]. Dostupné z: https://www.uoou.cz/urad/ds-1059/p1=1059

legislativních aktivit a zajišťování plnění požadavků vyplývajících z mezinárodních smluv a v neposlední řadě také přednáškové a osvětové činnosti.

Úřad působí nezávisle na jiných státních orgánech a řídí se pouze zákony a jinými právními předpisy. Zajištění nezávislosti je upraveno tak, že jeho činnost je financována ze samostatné kapitoly státního rozpočtu České republiky. Garance nezávislosti je dána také tím, že jmenování a odvolávání předsedy Úřadu a jeho inspektorů je v rukou prezidenta České republiky, který tak činí na návrh Senátu Parlamentu České republiky. Předseda Úřadu je jmenován na pět let, inspektoři jsou jmenováni na deset let a lze každého z inspektorů jmenovat opakovaně. Každý rok předkládá výroční zprávu o činnosti Úřadu Poslanecké sněmovně a Senátu Parlamentu České republiky a též i vládě České republiky.

Jednou z hlavních činností Úřadu je kontrolní činnost. Kontroly provádějí pouze inspektoři a pověření zaměstnanci na základě kontrolního plánu či na základě stížností a podnětů. Při sestavování kontrolního plánu věnují pozornost podnětům a stížnostem. Leckdy drobnost, na kterou stěžovatel v podání upozorní, může vést k odhalení závažných nedostatků při zpracování osobních údajů. Kontrolovanými jsou jak orgány státní správy či veřejnoprávní subjekty, tak i banky, podnikatelské subjekty, zdravotnická zařízení a další.[46] Kontroloři mají jasně daná práva pro výkon kontroly, mohou například nařídit správci a zpracovateli (případně jejich zástupcům), aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů.

Pokud Úřad objeví vážný nedostatek či chybu, může uložit správci pokutu. Ukládání správních pokut musí být účinné, přiměřené, ale zároveň odrazující. Správní pokuty se ukládají podle okolností každého jednotlivého případu. Za každé jednotlivé porušení nehrozí správci hned pokuta, ale správce může být nejprve upozorněn, že plánované operace zpracování pravděpodobně porušují Obecné nařízení. Pokud se jedná o závažné porušení Obecného nařízení, může být správci udělena pokuta. Výše pokut je rozdělena do dvou skupin dle porušení, jakého se správce dopustil. Pokutu lze udělit buď do výše 10 000 000 EUR (nebo až do 2% celkového ročního obratu skupiny, jde-li o podnik) nebo do výše 20 000 000 EUR (nebo až do 4% celkového ročního celosvětového obratu podniku). Rozdělení do dvou skupin odráží důležitost porušených povinností. Do nižší sazby spadá například porušení ustanovení týkající se záznamů o činnostech zpracování či posouzení vlivu na ochranu osobních údajů, zatímco do vyšší

[46] UOOU [online]. [cit. 17. 12. 2019]. Dostupné z: https://www.uoou.cz/informace-o-kontrolach/ds-1279/p1=1279

sazby jsou například zahrnuta porušení povinností upravujících zásady a zákonitosti zpracování, podmínky souhlasu se zpracováním osobních údajů atd.[47]

Také subjekt údajů má v rámci kontroly svá práva. Pokud vznikne subjektu údajů hmotná či nehmotná újma v důsledku porušení obecného nařízení ze strany správce či zpracovatele, má právo na úhradu újmy. Nejčastěji to bude znamenat obrátit se přímo s žádostí o náhradu na správce či zpracovatele, a pokud ten nebude dobrovolně plnit, bude se subjekt údajů muset obrátit na soud.[48]

[47] NEZMAR, L. *GDPR: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 43-44 s. ISBN 978-271-0668-4

[48] UOOU [online]. [cit. 5. 1. 2020]. Dostupné z: https://www.uoou.cz/11-sankce-pokuty/d-27287

3 Kamerové systémy

Jednou z oblastí, která je zavedením GDPR nejvíce ovlivněna je problematika kamerových systémů. Provoz kamer je neoddělitelně spjat s ochranou soukromí. Provozem kamerového systému se správce dostává do režimu Obecného nařízení. Ke zpracování dat ze záznamu kamer musí správce disponovat právním důvodem. Kamerový systém nelze instalovat na každém místě, ale správce musí pečlivě volit prostory, jejichž monitorování je nezbytné pro ochranu jeho majetku, ale i zdraví či života lidí, a zároveň tento zájem správce či třetích osob převažuje nad právem na ochranu soukromí člověka. V žádném případě nemá cenu koncipovat provozování kamerového systému na základě souhlasu, jelikož se nikdy nezaručí 100% souhlas všech osob. Souhlas je navíc právní důvod nestálý, protože je odvolatelný. V rámci zabezpečení se musí vyřešit i přístupová práva, tj. kdo bude moci se záznamy manipulovat.[49]

Provozování kamerového systému je považováno za zpracování osobních údajů podléhající povinnostem podle obecného nařízení, pokud je automatizovaně prováděn záznam monitorovaného veřejného prostoru a zároveň je účelem pořizovaných informací a záznamů využití k identifikaci fyzických osob v souvislosti s určitým jednáním.

Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu. Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým, na snímku zachyceným, jednáním. Kamerové sledování nesmí nadměrně zasahovat do soukromí. Kamerový systém je možno použít zásadně v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. lepším zabezpečením majetku). Dále je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (např. toalety, sprchy). Je-li kamerový systém využíván na pracovišti, musí provoz kamer a využití záznamu být v souladu s pracovněprávními předpisy. Je také třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými zájmy správce (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy

[49] ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 215-219 s. ISBN 978-80-7554-152-9

správce. Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. boj proti pouliční kriminalitě. Dále je třeba stanovit lhůtu pro uchovávání záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt nebo případně i dobu delší, v zásadě však nepřesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle zvláštního zákona. Po uplynutí této doby musí být vymazána. Pouze v případě existujícího bezpečnostního incidentu by měla být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu. Je třeba řádně zajistit ochranu snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním. Subjekt údajů musí být o užití kamerového systému a o tom, kdo jej provozuje, v převážné většině případů vhodným způsobem informován (např. nápisem umístěným v monitorované místnosti, vzor informační tabule tvoří přílohu č. 2 této práce).[50]

Povinností vyplývající z provozování kamerového systému je nutnost vyhotovit záznamy o činnostech zpracování. Tyto záznamy by měly obsahovat jméno a kontaktní údaje správce, účely zpracování údajů, popis kategorie údajů, příjemce, jimž jsou údaje zpřístupněny, lhůty pro výmaz, ale také technická a organizační bezpečnostní opatření. Záznamy musí být vyhotovovány písemně a správce je povinen je na požádání poskytnout dozorovému úřadu. Novou povinností je také ohlášení porušení zabezpečení či úniku dat dozorovému úřadu do 72 hodin od zjištění nedostatků.

Na příkladu kamerových systémů jsme si ukázali, jak funguje Obecné nařízení o ochraně osobních údajů v praxi. Bezesporu přináší pro správce vyšší náklady na zabezpečení dat a jejich evidenci, pravděpodobně i na personální obsazení, ale pro subjekty údajů je Obecné nařízení pákou na firmy, instituce, podniky, aby nemohly s jejich osobními údaji snadno nakládat, jako tomu bylo do května 2018. Subjekty údajů měly jen malou šanci řídit, kde všude a jak se s jejich osobními údaji nakládá, neboť každá firma, ať už se jedná třeba i o ten nejmenší internetový obchod, mohla po subjektu údajů žádat osobní data a bez jejich uvedení nebylo možné pro subjekt údajů službu podniku získat. Další nespornou kladnou změnou pro subjekty údajů je možnost odvolat

[50] UOOU [online]. [cit. 7. 1. 2020]. Dostupné z: https://www.uoou.cz/k-nbsp-provozovani-kamerovych-systemu/d-29535/p1=1099

svůj souhlas se zpracováním osobních údajů. Na příkladu kamerových systémů vidíme, že použití kamerového záznamu není relevantní, neboť souhlas se zpracováním osobních údajů může být kdykoli zrušený.

Teprve čas ukáže, zda aktuální podoba Obecného nařízení o ochraně osobních údajů bude dostačující, ale vzhledem k vývoji informačních technologií bude v budoucnu jistě potřeba její neustálá novelizace. Každopádně Obecné nařízení přineslo ochranu pro subjekty údajů v podobě, jaká tu doteď nebyla a domnívám se tvrdit, že budoucnost bude ve znamení ještě přísnější ochrany osobních údajů.

Z povinnosti vést záznamy o činnostech zpracování jsou vyloučeny podniky nebo organizace zaměstnávající méně než 250 osob. Nakládání se záznamy a doba jejich uchovávání se odvíjejí od účelu, pro jaký je záznam opatřován. Například při zachycení krádeže na kamerový systém by tyto záznamy měly být předány Policii České republiky, která má zákonné oprávnění zveřejňovat i audiovizuální záznamy a dále s nimi pracovat pro účely dopadení pachatele.[51]

Povinností správce je vedení záznamů o činnostech zpracování údajů.

3.1 Kamerový systém – specifikace

Kamerové systémy jsou souborem zařízení umožňujících monitorování zájmové oblasti. Skládá se z kamer, záznamového zařízení a dohledového pracoviště. Kamery zajišťují zdroj dat, záznamové zařízení tato data ukládá pro pozdější využití a dohledové pracoviště slouží ke sledování živého obrazu z jednotlivých kamer nebo přehrávání dříve uložených záznamů. Některé kamerové systémy mohou pracovat pouze jako online dohledový systém a záznamové zařízení pro své fungování nepotřebují. Vyžadují však pro své fungování obsluhu, která nepřetržitě sleduje živý obraz kamer a vyhodnocuje aktuální dění. Pro účely moderního kamerového systému se používají již výhradně IP kamery (nebo také digitální kamery). Jako dohledové pracoviště postačí počítač s monitorem, notebook, tablet nebo mobilní telefon. Záznamové zařízení je zpravidla tvořeno diskovým polem, jehož kapacita je přímo úměrná rozsáhlosti kamerového systému. Kamerové systémy je možné rozšířit i o další specifická zařízení jako externí IR přísvity, čidla, reproduktory nebo servery s programem pro inteligentní analýzu obrazu.[52]

Základní rozdělení kamerového systému je dle použití, a to vnitřní a vnější. Vnitřní kamery jsou určeny pro instalaci do interiéru, zpravidla chodeb, kanceláří nebo

[51] ŽŮREK, Jiří. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 220-222 s. ISBN 978-80-7554-152-9
[52] TINT.cz [online]. [cit. 7. 3. 2020]. Dostupné z: http://www.kamerove-systemy-tint.cz/

obchodů. Jejich konstrukce nemusí splňovat odolnost vůči vodě nebo nízkým teplotám a vnitřní kamery tak mohou být menší a méně nápadné. Některé vnitřní kamery typu kopule využívají takovou konstrukci, která umožňuje instalaci do podhledu. Taková kamera nenarušuje vzhled místnosti a zároveň je její tělo chráněno před neoprávněnou manipulací. Existují také speciální kamery s odděleným objektivem, který je s vlastním tělem kamery spojen až 12 metrů dlouhým kabelem. Lze je instalovat zcela skrytě například do rámu dveří, do konstrukce bankomatů nebo jiných míst, která vyžadují detailní záběr, ale zároveň neumožňují umístění klasické vnitřní kamery.

Venkovní kamery musí být konstruovány tak, aby odolaly vnějším vlivům. Měly by dosahovat odolnosti proti vodě a prachu dle standardu alespoň hodnoty IP66 a také odolnosti proti teplotním výkyvům. Kamera by měla být schopna fungovat v mrazu, ale i při vysokých teplotách. Běžně vnější kamery odolávají teplotám od -30°C do +50°C, některé venkovní kamery mají speciální konstrukci, která zajišťuje vyhřívání, případně chlazení a rozsah funkčních teplot může být ještě vyšší.[53]

Dále je také možné se setkat s kamerami, které jsou určeny do velmi náročných podmínek a kryt kamery dokáže odolat i chemikáliím nebo slané vodě.

3.2 Kamerový systém v bytovém domě

Tisíce každoročně vykradených bytů a také fakt, že se policii nedaří vyřešit více než dvě třetiny těchto případů, vede obyvatele bytových domů ke snaze zabránit zlodějům v krádežích různými bezpečnostními opatřeními. Za rok stačí zloději odcizit či poničit majetek za zhruba 450 milionů korun[54]. Jedním z opatření na ochranu je právě zavedení kamerového systému v bytovém domě. Bezpečnostní kamery nejčastěji chrání novou fasádu, výtahy, schránky, dveře a zvonková tabla. Kamery mají také psychologický efekt a pachatele odradí, pokud vidí, že jsou v objektu nainstalovány. Před samotným pořízením kamerového systému ale musí každé společenství vlastníků bytového domu pečlivě zvážit pro a proti instalace. Musí se zcela jasně vyjasnit otázky, zda je zavedení kamerového systému opravdu jediné správné řešení pro ochranu majetku. Dále je třeba si ujasnit, jaký přesný účel má zavedení kamerového systému v domě mít, neboť je nezbytné definovat legitimní účel zpracování osobních údajů, který se úzce pojí se zavedením kamerového systému.

[53] TINT.cz [online]. [cit. 7. 3. 2020]. Dostupné z: http://www.kamerove-systemy-tint.cz/
[54] idnes.cz [online]. [cit. 7. 2. 2020]. Dostupné z: https://www.idnes.cz/bydleni/stavba/kamerove-systemy-v-domech-sankce.A160130_115935_stavba_rez

„Jednou ze základních otázek zpracování osobních údajů prostřednictvím kamerových systémů v bytových domech je posouzení poměru mezi hodnotami, které mají být chráněny, na jedné straně (např. ochrana života a zdraví, ochrana majetku), a hodnotami, do kterých bude zasaženo, na straně druhé (ochrana soukromí). Každý, kdo hodlá instalovat a provozovat kamerový systém, musí posoudit, zda je zvolený prostředek (kamerový systém) způsobilý a potřebný k dosažení cíle (např. odradit či následně odhalit pachatele krádeže apod.) a vhodně jej kombinovat s dalšími prostředky (např. zamykání dveří, mříže apod.) tak, aby zvolené řešení nepřiměřeně nezasahovalo do práva na soukromí všech lidí, kteří se v prostorách bytového domu mohou pohybovat.“[55]

Každý, kdo bude kamerový systém provozovat, musí být schopen doložit potřebnost a užitečnost kamerového systému. Provozovatel kamerového systému v bytovém domě je i v průběhu provozu povinen kdykoliv prokázat, že kamerový systém jako prostředek k ochraně majetku a osob ve zvolené lokalitě je s ohledem na jistý zásah do soukromí osob vhodným řešením. Správce kamerového systému musí zvážit instalaci i z hlediska povahy prostor, které mají být sledovány – jestli se jedná o prostory, které jsou průchozí pouze příležitostně, anebo zda slouží jako bezprostřední přístup k bytům, v nichž obyvatelé domu mají nárok na nejvyšší míru soukromí. Prostory, jejichž sledování je nejvíce v souladu se zásadami účelného a přiměřeného zpracování osobních údajů jsou sklepy, půdy a vchody do nich, garáže, kočárkárny, kolárny, prostory dopisních schránek, vnější plášť budovy a jeho bezprostřední okolí. Podobně jsou také obvykle posuzovány vstupní dveře do domu, vstupní chodby k výtahům a schodištím i výtahy a schodiště. Ve všech prostorách je však třeba dbát na pečlivé nastavení kamerového systému, zejména úhlu záběru kamery ve vztahu k celkovému rozsahu snímaných prostor tak, aby současně nebyla snímána jiná místa, v nichž by sledováním bylo více zasaženo soukromí obyvatel či návštěvníků domu.[56]

Co se týče jednotlivých bytů v bytovém domě, tak při nastavení kamerového sytému na konkrétní byty může docházet k závažným zásahům do práva na ochranu soukromého a osobního života a lze jej uskutečnit jen ve výjimečných a odůvodněných případech, a to se souhlasem obyvatel dotčených bytů.

[55] UOOU [online]. [cit. 7. 2. 2020]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=18866&n=stanovisko%2Dc%2D1%2D2016%2Dumisteni%2Dkamerovych%2Dsystemu%2Dv%2Dbytovych%2Ddomech

[56] UOOU [online]. [cit. 7. 2. 2020]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=18866&n=stanovisko%2Dc%2D1%2D2016%2Dumisteni%2Dkamerovych%2Dsystemu%2Dv%2Dbytovych%2Ddomech

Správce je povinen před zahájením zpracování informovat obyvatele domu o zamýšlené instalaci kamerového systému. Dostatečné pro splnění této povinnosti je, když správce informuje obyvatele prostřednictvím schůze shromáždění společenství vlastníků jednotek a následně vyvěsí či rozešle informaci všem obyvatelům domu. Obsahem informování by mělo být, kdo a jakým způsobem bude údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, správce také musí informovat o právu přístupu k osobním údajům, právu na opravu osobních údajů, a zda je poskytnutí dobrovolné či nedobrovolné. Správce kamerového systému má také oznamovací povinnost vůči Úřadu pro ochranu osobních údajů. Správce byl do doby zavedení GDPR povinen před zahájením zpracování údajů písemně oznámit Úřadu zamýšlené zpracování osobních údajů, toto nařízení je ale nyní nahrazeno a místo registrace na UOOU má v souvislosti s provozováním kamerového záznamu správce povinnost vést záznamy o činnostech zpracování[57].

Souhlas se zpracováním osobních údajů, který je třeba mít pro provozování kamerového systému v bytových domech je možný získat několika způsoby. Prvním je souhlas se zpracováním osobních údajů jakožto právní titul, ovšem takový souhlas je možné následně odvolat. Druhým způsobem je udělení souhlasu od všech obyvatel domu, ale to přináší komplikace v případech, kdy se mění majitelé či nájemníci bytů a je nutné neustále souhlasy doplňovat o nově příchozí. Dalším případem se jeví tzv. souhlas většiny, kdy se společenství vlastníků dohodne na zřízení kamerového systému, ale tento souhlas není kvalifikovaným souhlasem dotčených osob ve smyslu zákona o ochraně osobních údajů, jedná se pouze o faktor zdůvodňující potřebnost kamerového systému.[58]

„V případě dalších osob, které do bytového domu budou přicházet nepravidelně, resp. nepředvídatelně, je správce povinen splnit informační povinnost alespoň umístěním informačních tabulek u všech vstupů do sledovaných prostor (vč. vstupu do výtahu). Informační tabulka musí obsahovat alespoň informaci, že prostor je sledován kamerovým systémem, musí zde být uveden správce – provozovatel kamerového systému, resp. kontaktní osoba nebo sdělení, kde bude subjektu údajů poskytnuta (např. v písemné podobě) kompletní informace o zpracování v rozsahu požadovaném zákonem.“[59]

[57] WebDOMU.cz [online]. [cit. 7. 2. 2020]. Dostupné z: https://webdomu.cz/s/aktuality/kamerovy-system-v-bytovem-dome
[58] UOOU [online]. [cit. 7. 2. 2020]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=18866&n=stanovisko%2Dc%2D1%2D2016%2Dumisteni%2Dkamerovych%2Dsystemu%2Dv%2Dbytovych%2Ddomech
[59] UOOU [online]. [cit. 7. 2. 2020]. Dostupné z: https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=18866&n=stanovisko%2Dc%2D1%2D2016%2Dumisteni%2Dkamerovych%2Dsystemu%2Dv%2Dbytovych%2Ddomech

Kamery, celou přenosovou soustavu a záznamové zařízení je nutné náležitě zabezpečit, aby nemohlo dojít k úniku záznamu. Zákon ukládá správcům a zpracovatelům povinnost přijmout a dokumentovat řadu bezpečnostních opatření, které mají předcházet neoprávněnému přístupu k osobním údajům, jejich změně, zničení nebo ztrátě, neoprávněným přenosům zpracování, nebo zneužití. Úřad pro ochranu osobních údajů určil, že takovým opatřením je zejména zabezpečení přenosové soustavy a záznamového zařízení a vnitřní zabezpečení. Také všechny přístupy k záznamům musí být evidovány, aby bylo zřejmé, kdo, kdy a z jakého důvody do záznamu nahlížel. Jakýkoliv svévolný přístup ke kamerovému systému a jeho záznamům mimo stanovený bezpečnostní režim je deliktem, za který může být uložena pokuta až 5 mil. Kč. Přístup k systému má být zabezpečený heslem a zařízení smějí obsluhovat pouze určené osoby. Podle úřadu by doba, kdy se záznamy uchovávají, neměla překročit 14 dnů. Doba uchovávání záznamů je stanovena tak, aby nepřesáhla dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možno dále prošetřit a zajistit další nezbytné informace, potřebné například k předání záznamu příslušným orgánům či pojišťovně. Takovou dobou je obvykle nejvýše 7 dnů, v případě příležitostně navštěvovaných prostor až 14 dnů. V odůvodněných případech může správce dobu prodloužit.

3.3 Kamerový systém ve školách

Zavádění kamerových okruhů do vnitřních i venkovních prostor školních institucí je do značné míry kontroverzní a eticky složité téma a i pohled na něj se v očích vedení školy, pedagogů i rodičů v čase mění. Zatímco když byly kamerové systémy implementovány před deseti lety, nezřídka vznikaly protestní rodičovské petice, v současné době nejsou vzácné situace, kdy sami rodiče po ředitelích škol vyžadují vybudování kamerového systému.[60]

Stejně tak jako v případě zavedení kamerového systému v obytných domech je i ve školách nejprve dobré pečlivě zvážit účel, kvůli kterému by byl kamerový systém zaveden. Nestačí stanovit jako účel ochranu majetku a prevenci kriminality, to jsou pouze obecné účely, za adekvátní účel je považováno například to, pokud k ohrožení majetku nebo zdraví již došlo a selhaly všechny dosavadní metody pedagogického dozoru, pak je na místě zvážit nasazení vyššího stupně ostrahy osob a majetku, kam nasazení kamerového systému nepochybně patří. Je také třeba stanovit způsob provozování

[60] Secutek [online]. [cit. 27. 2. 2020]. Dostupné z: https https://secutek.cz/blog/47/kamerove-systemy-ve-skolach-stale-beznejsi-praxe-.html

kamerového systému, neboť *„musí být nastaven takový režim, který by s ohledem na zájmy správce nebo jeho právní odpovědnost co nejméně omezoval jiná práva. Jednotlivé části systému tak mohou pracovat zcela nezávisle a v jiném časovém režimu, kdy například kamery v šatnách se mohou spouštět se začátkem vyučování a naopak kamery ve společných prostorách (chodbách, jídelnách a pod) v době, kdy zde žáci nepracují, a je na místě chránit majetek správce před nahodilým útokem neznámého pachatele.“*[61] Nepřijatelné je třeba kameru instalovat na toalety, naopak nejčastěji kamery dohlížejí na chodby, šatny nebo počítačové učebny. V současné době se objevují dokonce hlasy volající po zavedení kamer i do tříd, což je z právního, pedagogického i etického hlediska ještě o poznání problematičtější a diskutabilnější otázkou, než v případě zabezpečení dohledu nad společnými prostory vzdělávací instituce. Jedním z argumentů je mimo jiné zvyšování kvality výuky.[62]

Další oblast, kterou je třeba zvážit je systém záznamového zařízení, zde musí být jasně stanoven čas pro uchovávání informací. Musí být vymezena jasná pravidla, kdo vše má přístup ke kamerovým záznamům vč. manipulace s nimi, jak dlouho se budou záznamy uchovávat a jak k nim mohou přistupovat i samotné subjekty osobních údajů. Co ale není ve školském zařízení doporučeno, je bezpečnostní pult, kde pověřená osoba neustále sleduje dění na kamerách, neboť by se mohlo jednat o neodůvodněné sledování nejen žáků, ale také pedagogických pracovníků. Sledování osob pak nespadá pod ochranu osobních údajů, ale spíše pod ochranu osobnosti podle občanského zákoníku. A v neposlední řadě je třeba vyřešit souhlas se zpracováním osobních údajů žáků, kteří ještě nejsou plnoletí, tento souhlas musí dát jejich zákonní zástupci. A při plánování nasazení kamerového systému musí být vypracovaný projekt rozmístění kamer vč. stanovení časového režimu pro snímání jednotlivých prostorů.[63]

Neexistuje přesná statistika o tom, jaké procento škol u nás je vybaveno kamerovým systémem. Odhaduje se, že aktuálně více než 50 % středních škol a zhruba třetina škol základních nějakým takovým systémem disponuje. Zřejmé je, že jejich podíl neustále narůstá, přičemž jistou roli hraje i podpora některých městských částí či radnic přispívajících školám na jejich pořízení. Vedle pořizování kamerových systémů školy stále v hojnějším počtu využívají také čipy, případně turnikety s cílem zabránit vstupu osob, jež nemají v dané škole co pohledávat. Pomyslnou odvrácenou stranou mince stojící

[61] UOOU [online]. [cit. 27. 2. 2020]. Dostupné z: https://www.uoou.cz/files/tk_2006-11-27_3.pdf
[62] Secutek [online]. [cit. 27. 2. 2020]. Dostupné z: https https://secutek.cz/blog/47/kamerove-systemy-ve-skolach-stale-beznejsi-praxe-.html
[63] GDPR do škol [online]. [cit. 27. 2. 2020]. Dostupné z: http://gdprdoskol.cz/bezpecnostni-kamery-ve-skolach-ochrana-osobnich-udaju/

proti těžko zpochybnitelným přínosům představují třeba všudypřítomné riziko zneužití záznamu nebo osobních údajů, obavy ze ztráty soukromí, možného pocitu narušení důvěry mezi pedagogem a žáky i mezi dětmi navzájem.[64]

Závěrem je třeba říct, že pokud se školy rozhodnout k nasazení bezpečnostních kamer, musí pamatovat, že takové jednání je regulováno předpisy na ochranu osobních údajů a je třeba splnit určité povinnosti. Kamerové systémy jsou velkým zásahem do soukromí dětí studujících v dané škole a učitelů, kteří v ní učí. Z tohoto důvodu ÚOOÚ opakovaně zmiňuje, že k používání kamer by se mělo přistoupit až ve chvíli, kdy monitorování prostorů nelze zajistit jinými prostředky a zároveň musí být možné prokázat, že opravdu nebylo možné bezpečnost zajistit méně invazivními prostředky. Kamerové systémy mohou být provozovány například tak, že budou pouze na vnějším plášti budovy nebo budou-li ve vnitřních prostorech, tak budou zapnuty pouze v době, kdy v daných prostorech nemá nikdo být (např. šatny – během vyučování nebo v pozdějších večerních hodinách po jeho úplném skončení) a nebude tak docházet k masivnímu monitorování osob nebo nainstalujete kamerové systémy, které budou tzv. bez záznamu.[65]

3.4 Kamerové systémy ve firmách

Zavedením kamerového systému zaměstnavatel výrazně zasahuje do osobních práv zaměstnanců, a tak jsou zaměstnavatelé vždy povinni respektovat pravidlo, že mohou své zaměstnance otevřeně nebo skrytě sledovat na pracovištích a ve společných prostorách pouze tehdy, pokud je dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Při sledování nesmí zaměstnavatel nepřiměřeně zasahovat do práv zaměstnanců na ochranu jejich soukromého a osobního života. To znamená, že zaměstnavatel nemůže své zaměstnance v žádném případě sledovat v šatně nebo na toaletách a dalších podobných místech.

Problematika bezpečnostních kamer není z pohledu práva složitá. Je však nezbytné udělat vždy základní analýzu podoby zamýšleného bezpečnostního systému ve vztahu k právním požadavkům a tomu následně přizpůsobit administrativní agendu požadovanou právními předpisy.

[64] Secutek [online]. [cit. 27. 2. 2020]. Dostupné z: https https://secutek.cz/blog/47/kamerove-systemy-ve-skolach-stale-beznejsi-praxe-.html
[65] GDPR do škol [online]. [cit. 27. 2. 2020]. Dostupné z: http://gdprdoskol.cz/bezpecnostni-kamery-ve-skolach-ochrana-osobnich-udaju/

Zavedení kamerového systému ve firmě má svá jasná pravidla, zaměstnavatel musí své zaměstnance informovat o tom, v jakém rozsahu a pro jaký účel dochází k pořizování kamerového záznamu, kdo a jakým způsobem bude záznamy zpracovávat a kdo k nim může mít přístup, jakož i právech o právech zaměstnanců pro případ zpracování osobních údajů v rozporu se zákonem nebo v rozporu s ochranou soukromého a osobního života. Zaměstnavatel také musí zabezpečit zařízení kamerového systému i pořízené záznamy proti neoprávněnému přístupu cizích osob.

Při použití kamerových systémů ke sledování osob a záznamům těchto osob platí, že musí být nezbytné pro naplnění konkrétního účelu a musí být přiměřené vzhledem k okolnostem a k ochraně soukromí těchto osob. Je třeba maximálně respektovat soukromí a oprávněné zájmy osob, např. kupujících v obchodním centru, řidičů v podzemních garážích a podobně.

Pokud by zaměstnavatel chtěl umístit kamery přímo nad pracoviště svých zaměstnanců narazil by nejen na ochranu osobních údajů, ale i na zákoník práce, neboť zaměstnavatelé nesmí, až na odůvodněné výjimky a zvláštní případy popsané v Zákoníku práce, sledovat své zaměstnance.[66]

3.5 Městské kamerové systémy

Jedná se o kamerové systémy zřízené a provozované městy nebo obcemi, které slouží pouze pro potřeby Policie ČR. Jednotlivé kamery jsou instalované na vybraných rizikových místech, kde se nejčastěji pohybují obyvatelé a návštěvníci měst, kde jsou koncentrovány kulturní, komerční a společenské instituce a kde jsou dopravní uzly měst, např. náměstí, pěší a obchodní zóny, parkoviště, autobusové či vlakové nádraží, sídliště, pro zajištění bezpečnosti a snížení kriminality. Základní charakteristikou provozování a využívání městských kamerových systémů je tedy jejich preventivní funkce, tj. vytváření bezpečných zón v exponovaných lokalitách. Městské kamerové systémy mohou monitorovat pouze veřejné prostranství, tzn. náměstí, ulice, tržiště, chodníky, veřejnou zeleň, parky, a další prostory přístupné každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru.[67] Riziková místa měst a obcí vhodná k nasazení kamerového systému stanovuje na základě podrobných analýz Policie České republiky.

[66] BusinessInfo.cz [online]. [cit. 28. 2. 2020]. Dostupné z: http https://www.businessinfo.cz/clanky/gdpr-ovlivni-take-kamerove-systemy-ve-firmach-na-co-si-podniky-musi-dat-pozor

[67] Ministerstvo vnitra České republiky [online]. [cit. 8. 3. 2020]. Dostupné z: https://www.mvcr.cz/clanek/kamerove-systemy.aspx

Záznamy ze všech kamerových systémů města jsou pomocí speciálního softwaru přenášeny a uchovávány na policejní stanici, kde mohou strážníci nejen hledat v záznamech (např. důkazní materiál), ale také živě sledovat a případně ihned zasáhnout.

Obecně bohužel není na městské kamerové systémy pohlíženo občany příliš věrohodně a často jsou všudypřítomné kamery vnímány jako oči tzv. „velkého bratra“. Negativní vnímání je spojeno především s obavou, jak je nakládáno s osobními údaji občanů, kteří jsou monitorovány apod. Tyto obavy ale rozhodně nejsou na místě. Nejenže musí být každý informován o faktu, že je v daném místě monitorován, ale především musí město při používání městského kamerového systému dodržovat ustanovení o ochraně osobních údajů. Navíc veškeré záznamy jsou spravovány státní či městskou policií a veškeré zveřejňování osobních údajů v souvislosti se zajištěním veřejného pořádku může být provedeno jen se souhlasem osob, o jejichž údaje se jedná.[68]

Do městského kamerového systému lze integrovat i další systémy. Výhodou rozšířeného systému je vzájemné sdílení informací. Do městského kamerového systému je tak možné připojit kamery dopravního podniku, dopravní a rychlostní kamery a kamery městských částí. Městský kamerový systém v současné době tvoří robustní řešení schopné obsluhovat i tisíce kamer. Při řešení incidentů systém umožňuje přístup k živému obrazu i k záznamu. Přístup k záznamu má na základě platné legislativy pouze Policie ČR a Městská policie. Záznam z kamer se uchovává až 30 dní.[69]

O tom, že je veřejné prostranství monitorováno, musí být občané města a jeho návštěvníci dostatečně a srozumitelně informováni, například pomocí informační tabule s textem *"Tento prostor je pod nepřetržitým dohledem kamer městské policie/ Policie ČR"*.

[68] KaP systém.cz [online]. [cit. 8. 3. 2020]. Dostupné z: http://www.kapsystem.cz/mestske-kamerove-systemy/

[69] ELTODO.cz [online]. [cit. 8. 3. 2020]. Dostupné z: https://www.eltodo.cz/produkty-a-sluzby/kamerove-systemy/mestske-kamerove-systemy/

4 Praktický příklad – Městský kamerový systém Třeboň

Město Třeboň uvedlo do provozu městský kamerový systém v roce 2004. Na financování kamerového systému město využilo státní dotaci z fondů Ministerstva vnitra. Dotace státu činila 1 300 000,- Kč, k tomu přispělo Město Třeboň částkou 215 000,-Kč. Pro realizaci projektu bylo vypsáno výběrové řízení, kterého se zúčastnilo 10 odborných firem z celé republiky.

Po vyhodnocení všech bezpečnostních kritérií bylo v první fázi realizace kamerového systému vybráno 8 nejfrekventovanějších míst ve městě. A uvažovalo se i o zřízení mobilního kamerového bodu dle aktuálních potřeb, který ale zatím nebyl realizován. Monitorovací středisko, vlastní mozek kamerového systému, je umístěno na služebně Městské policie a obsluhují jej vybraní specialisté. Díky technickému opatření mohou pořizovaný záznam sledovat i příslušníci Policie ČR na místním obvodním oddělení.[70]

Vedení Městské policie občany ujistilo, že v žádném případě nebudou porušována jejich práva. Snímána budou prostranství, která snímaná smějí být. Obsluha je poučena o podmínkách provozu kamerového systému a dopředu bylo jasně oznámeno, že ani drobné porušení zákonných podmínek ze strany obsluhy nebude tolerováno. Pracovat se zaznamenanými údaji mohou pouze vybraní specialisté.

Vrchní strážník Městské policie uvedl, že tam, kde se kamery umístily, se bezpečnostní a veřejně-pořádková situace zlepšila. Díky kamerám v Třeboni dokázali pochytat zloděje, zabránit vandalismu případně přímo při činu zadržet pachatele vandalských činů a tím zabránit škodám na veřejném i soukromém majetku. Odhalili jak pachatele trestných činů, tak se jim díky kamerovému systému podařilo objasnit dopravní nehody, zachytit pohyb osob porušujících zákony či zadržet osoby při porušování veřejného pořádku. Díky kamerám také dokázali včas pomoci i lidem, kteří měli vážné zdravotní problémy či se dostali do jiné kritické situace.[71]

Občané měli od začátku největší obavy z toho, aby nebyla narušena jejich svoboda, aby si na ně město nevytvořilo jakéhosi „velkého bratra“. Ale tyto obavy nebyly namístě. Kamerový systém může obsluhovat pouze úzký okruh vybraných operátorů seznámených se všemi podmínkami pro jeho provozování. S pořízenými záznamy může pracovat jen několik vybraných pracovníků, kterým to legislativa umožňuje. Kamerový

[70] Město Třeboň.cz [online]. [cit. 15. 3. 2020]. Dostupné z: https://www.mesto-trebon.cz/cz/mesto-3/mestska-policie-10/kamerovy-system-2/historie-kameroveho-systemu-v-treboni.html
[71] Město Třeboň.cz [online]. [cit. 15. 3. 2020]. Dostupné z: https://www.mesto-trebon.cz/cz/mesto-3/mestska-policie-10/kamerovy-system-2/kamery-ano-ci-ne.html

systém má i svá technická omezení, aby se zabránilo narušení soukromí obyvatel města. Jedním z omezení systému je takzvané "vymaskování" všech oken či prostor, kam se kamery dívat nesmějí. V praxi to znamená, že do žádného okna či prostoru " za zeď " kamery prostě nevidí, neboť při natočení se do těchto míst obraz na monitorech zmizí a ani operátor nemá technickou možnost toto omezení změnit.

Další z obav obyvatel města bylo, aby kamerový systém nenahradil strážníky. Ani tato obava se nepotvrdila. Pořízení kamerového systému nemělo vliv na počet strážníků Městské policie. Stav strážníků se nesnížil ani nezvýšil, kamery obsluhují operátoři stálé služby. Nelze proto hovořit o přesunutí strážníků od monitoringu do ulic, pouze stoupla náročnost práce operátorů stálé služby a musím konstatovat, že jsou velmi vytíženi. Na druhou stranu pořízení kamerového systému nemůže být ani důvodem ke snížení aktivity strážníků v ulicích. Naopak, kamery se staly pomocníkem strážníků i policistů v jejich činnosti.

Nahrávání záznamů je stanoveno na 7 až 10 dní v závislosti na jejich velikosti, poté jsou automaticky smazány. Jiná situace nastává, pokud si záznamy vyžádá městská, státní či kriminální policie, ty jsou potom archivovány po dobu 3 měsíců. Záznamy z kamerového systému mohou sloužit i jako důkaz při prokazování viny. Záznamy využívají orgány činné v trestním řízení, vyžadují je i soudy. Často záznam pomáhá při objasňování přestupků nebo trestných činů, pomáhá také například při objasňování dopravních nehod.[72]

[72] Město Třeboň.cz [online]. [cit. 15. 3. 2020]. Dostupné z: https://www.mesto-trebon.cz/cz/mesto-3/mestska-policie-10/kamerovy-system-2/rozhovor-s-operatorkou-kameroveho-systemu.html

Závěr

Ochrana osobních údajů nemá v ČR dlouhou existenci. První zákon, který upravoval ochranu osobních údajů byl datován rokem 2000. Od listopadové revoluce v roce 1989 až do roku 2000 si česká společnost vůbec nepřipouštěla nutnost či potřebu právní úpravy v této oblasti. Vstupem ČR do EU v roce 2004 bylo nutné se v oblasti ochrany osobních údajů ještě více přiblížit právu EU. Zákon o ochraně osobních údajů byl kompatibilní s právem EU (se Směrnicí č. 95/46/ES a Úmluvou č. 108) a tento zákon pak v květnu 2018 vystřídalo Obecné nařízení o ochraně osobních údajů, neboli GDPR (General Data Protection Regulation).

Cílem Obecného nařízení je přizpůsobení právního rámce ochrany osobních údajů dnešní době, dosažení větší jednoty právního rámce ve všech zemích, na které dopadá, posílení práv subjektu údajů a v neposlední řadě je snahou dosáhnout sjednoceného výkladu Obecného nařízení a dozoru jednotlivými dozorovými úřady.

Cílem práce bylo ukázat problematiku ochrany osobních údajů z hlediska právní úpravy, objasnit její vývoj, smysl a představit nové nařízení o ochraně osobních údajů, tedy Obecné nařízení o ochraně osobních údajů a ukázat na příkladu kamerových systémů, jak ovlivňuje a případně omezuje jejich zavádění. Hlavním důvodem, proč nařízení vzniklo, je skutečnost, že stále více osobních údajů se přenáší na internet. Lidé si mnohdy ani neuvědomují, jakým rizikům se vystavují tím, že vloží citlivé informace do nějakého systému. GDPR vrací rozhodování o tom, do jaké míry mohou společnosti a instituce zacházet s osobními údaji, do rukou lidí. Každá fyzická osoba by si měla uvědomit svá práva. A následně pak rozhodovat o tom, k čemu mohou být její osobní údaje využívány a k čemu ne. Rovněž firmy a instituce, které s těmito daty pracují, nevěnují dostatečnou pozornost jejich zabezpečení, často dochází k únikům a následnému zneužití osobních dat třetí stranou.

V práci se autor věnoval jak kamerovým systémům ve firmách, tak ve školách i městskými kamerovými systémy. Na příkladu z praxe ukázal, jaký byl vývoj a jak funguje městský kamerový systém v Třeboni.

Při zavádění kamerového systému ať už se jedná o firmy, školy, města, se nejvíce mluví o strachu ze ztráty soukromí a osobní svobody. Praxe ukazuje, že zavedení kamerového systému přináší více užitku, než omezení občanů. Městské kamerové systémy pomohly odhalit pachatele trestných činů, objasnit dopravní nehody, zachytit pohyb osob porušujících zákony či zadržet osoby při porušování veřejného pořádku, ale i díky nim policisté dokázali včas pomoci i lidem, kteří měli vážné zdravotní problémy

či se dostali do jiné kritické situace. Firemní a školní kamerové systémy pomohly s problémem vandalismu, krádeží, vstupu nepovolaných osob či v případě škol s potlačením šikany. Ale ani kamery nejsou všemocné, kamera nedokáže vidět za roh, ani nedokáže monitorovat několik míst najednou. Přesto operativnost i možnost prohlížení záznamu pořízeného při monitoringu má nespočet výhod. Jedinou obavou obyvatel tedy zůstává vnímání osobní svobody občana a pocit ohrožení jeho práv, ale to je díky GDPR právně ošetřeno a nelze s žádnými osobními údaji, ani kamerovým záznamem libovolně nakládat, natož ho jakkoli zneužít.

Seznam základní literatury

Literární zdroje:

1. JANEČKOVÁ, E. *GDPR Praktická příručka implementace.* Praha: Wolters Kluwer ČR, a.s., 2018. 136s. ISBN 978-80-7552-248-1.
2. KUČEROVÁ, A; BARTÍK, V; PECA, J; NEUWIRHTH, K; NEJEDLÝ, J. *Zákon o ochraně osobních údajů - komentář.* 1. vyd. Praha: C.H.Beck, 2003. 387 s. ISBN: 80-7179-762-6
3. MATOUŠOVÁ, M. a kol. *Ochrana osobních údajů v otázkách a odpovědích*. 1. vyd. Praha: ASPI, a.s., 2004. 160s. ISBN 80-7357-037-8
4. MATOUŠOVÁ, M.; HEJLÍK, L. *Osobní údaje a jejich ochrana*. 2. vyd. Praha: ASPI, a.s., 2008. 196 s. ISBN 978-80-7357-322-5
5. NEZMAR, L. GDPR*: Praktický průvodce implementací.* Praha: Grada Publishing, 2018. 301 s. ISBN 978-271-0668-4
6. NONNEMANN, F.; LIDINSKÝ, V.; MAŠÍN, D. Praktická příručka GDPR pro Správce, Zpracovatele a Pověřence ochrany osobních údajů. Praha: Nakladatelství Klika, 2018. 144 s. ISBN 978-80-88298-10-6.
7. ŽŮREK, J. *Praktický průvodce GDPR*. Olomouc: Anag, 2018. 344 s. ISBN 978-80-7554-152-9

Elektronické zdroje:

1. BusinessInfo.cz [online]. [cit. 28. 2. 2020]. Dostupné z: https://www.businessinfo.cz/clanky/gdpr-ovlivni-take-kamerove-systemy-ve-firmach-na-co-si-podniky-musi-dat-pozor
2. ELTODO.cz [online]. [cit. 8. 3. 2020]. Dostupné z: https://www.eltodo.cz/produkty-a-sluzby/kamerove-systemy/mestske-kamerove-systemy/
3. GDPR.cz [online]. [cit. 18. 12. 2019]. Dostupné z: https://www.gdpr.cz/blog/souhlas/
4. GDPR do škol [online]. [cit. 27. 2. 2020]. Dostupné z: http://gdprdoskol.cz/bezpecnostni-kamery-ve-skolach-ochrana-osobnich-udaju/
5. GDPRsoulutions.cz [online]. [cit. 15. 12. 2019]. Dostupné z: https://www.gdprsolutions.cz/automaticke-zpracovani-profilovani/
6. idnes.cz [online]. [cit. 7. 2. 2020]. Dostupné z: https://www.idnes.cz/bydleni/stavba/kamerove-systemy-v-domech-sankce.A160130_115935_stavba_rez

7. KaP systém.cz [online]. [cit. 8. 3. 2020]. Dostupné z: http://www.kapsystem.cz/mestske-kamerove-systemy/
8. Město Třeboň.cz [online]. [cit. 15. 3. 2020]. Dostupné z: https://www.mesto-trebon.cz/cz/mesto-3/mestska-policie-10/kamerovy-system-2/kamery-ano-cine.html
9. Ministerstvo vnitra České republiky [online]. [cit. 8. 3. 2020]. Dostupné z: https://www.mvcr.cz/clanek/kamerove-systemy.aspx
10. QCOM [online]. [cit. 5. 12. 2019]. Dostupné z: http://www.qcom.cz/systemy-rizeni/gdpr/proc-vzniklo-gdpr/
11. Secutek [online]. [cit. 27. 2. 2020]. Dostupné z: https https://secutek.cz/blog/47/kamerove-systemy-ve-skolach-stale-beznejsi-praxe-.html
12. TINT.cz [online]. [cit. 7. 3. 2020]. Dostupné z: http://www.kamerove-systemy-tint.cz/
13. UOOU [online]. [cit. 27. 2. 2020]. Dostupné z: https://www.uoou.cz/files/tk_2006-11-27_3.pdf
14. WebDOMU.cz [online]. [cit. 7. 2. 2020]. Dostupné z: https://webdomu.cz/s/aktuality/kamerovy-system-v-bytovem-dome

Seznam příloh

I. Vzor souhlasu se zpracováním osobních údajů

II. Informační tabule: Prostor je střežen kamerovým systémem

Souhlas se zpracováním osobních údajů

1. Udělujete tímto souhlas společnosti ……. , se sídlem ……., IČ: ……., zapsané ve veřejném rejstříku vedeném u ……. soudu v ……., oddíl …, vložka ……. (dále jen „Správce“), aby ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „Nařízení“) zpracovávala tyto osobní údaje:
   - jméno a příjmení
   - název společnosti
   - e-mail
   - telefonní číslo
   - …….

2. Jméno, příjmení, název společnosti, telefonní číslo a e-mail je možné zpracovat na základě Vámi uděleného souhlasu a je nutné zpracovat za účelem ……. . Tyto údaje budou Správcem zpracovány po dobu … let.

3. ……

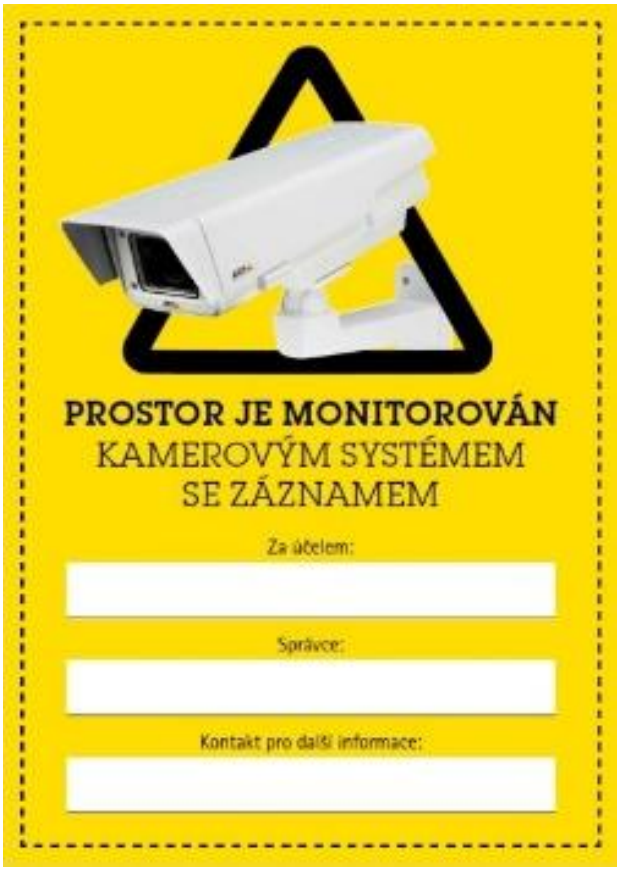
4. V případě cookies: Správce shromažďuje na svých webových stránkách následující soubory cookies:

Typ	**Název**	**Účel**	**Expirace**	**Přístup k informacím**
Např. systémová	*Např. Abcde*	*Např. Tato cookie se používá k ukládání dat důležitých pro fungování…*	*Např. Do uzavření okna prohlížeče*	*Např. jde o cookie z našeho webu*

5. S výše uvedeným zpracováním udělujete svůj výslovný souhlas. Poskytnutí osobních údajů je dobrovolné. Souhlas lze vzít kdykoliv zpět, a to například zasláním emailu nebo dopisu na kontaktní údaje společnosti ……

6. Zpracování osobních údajů je prováděno Správcem, osobní údaje však pro Správce mohou zpracovávat i tito zpracovatelé:
   a. Poskytovatel softwaru …….
   b. Agentura……..
   c. Případně další poskytovatelé zpracovatelských softwarů, služeb a aplikací, které však v současné době společnost nevyužívá.

7. Vezměte, prosíme, na vědomí, že podle Nařízení máte právo:
   - vzít souhlas kdykoliv zpět,
   - požadovat po nás informaci, jaké vaše osobní údaje zpracováváme, žádat si kopii těchto údajů,
   - vyžádat si u nás přístup k těmto údajům a tyto nechat aktualizovat nebo opravit, popřípadě požadovat omezení zpracování,
   - požadovat po nás výmaz těchto osobních údajů,
   - na přenositelnost údajů,
   - podat stížnost u Úřadu pro ochranu osobních údajů nebo se obrátit na soud.


PROSTOR JE MONITOROVÁN
KAMEROVÝM SYSTÉMEM
SE ZÁZNAMEM
Za účelem:
Správce:
Kontakt pro další informace: