Univerzita Palackého v Olomouci
Právnická fakulta

Jan Kotrba

Obecné nařízení o ochraně osobních údajů (GDPR) a vybrané aplikační problémy

Diplomová práce

Olomouc 2019

Prohlášení

Prohlašuji, že jsem diplomovou práci na téma Obecné nařízení o ochraně osobních údajů (GDPR) a vybrané aplikační problémy vypracoval samostatně a citoval jsem všechny použité zdroje.

V Praze dne 14. 1. 2019 ……

Jan Kotrba

Poděkování

Zde bych rád poděkoval panu **doc. JUDr. Václavu Stehlíkovi, LL. M, Ph. D**, za jeho odborné vedení při zpracování této diplomové práce a také mé matce za podporu během studia.

Obsah

Seznam použitých zkratek

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

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

SDEU..... Evropský soudní dvůr

EHP..... Evropský hospodářský prostor

ÚOOU..... Úřad pro ochranu osobních údajů

EU..... Evropská unie

Informační zákon..... zákon č. 106/1999, o svobodném přístupu k informacím

IT..... Informační technologie

Skupina WP29..... Pracovní skupina 29, předchůdce dnešního Evropského sboru pro ochranu osobních údajů

USA..... Spojené státy Americké

Komise..... Evropská komise

MŠMT..... Ministerstvo školství mládeže a tělovýchovy

MV ČR..... Ministerstvo vnitra

BDSG..... Bundesdatenschutzgesetz

NOZ..... zákon č. 89/2012 Sb., občanský zákoník

1 Úvod

GDPR (Obecné nařízení o ochraně osobních údajů fyzických osob) bylo v roce 2018 jedním z nejdiskutovanějších témat v oblasti právní vědy. Téma diplomové práce jsem si zvolil z důvodu aktuálnosti tohoto tématu a zároveň i z důvodu mé praxe v této oblasti. V rámci působení u několika malých organizací jako pověřenec pro ochranu osobních údajů bych rád praktickou stránku uplatnil i v teoretické rovině. V první kapitole chci v malém měřítku zmínit vývoj právní úpravy ochrany osobních údajů, důvody přijetí nařízení na úrovni EU a také nastínit možné dopady na český právní řád.

V další kapitole se chci zaměřit více prakticky a to hlavně na orgány veřejné moci (zejména obce, mateřské školky atd.). V první podkapitole chci nadefinovat povinnosti, které jim ukládá obecné nařízení, zhodnotit význam povinností za použití technických a organizačních opatření a zda je složité těmto povinnostem dostát.

V podkapitole, která se týká správců a zpracovatelů, ve vzájemných souvislostech se opět zaměřím prakticky na konkrétní obce. Vybral jsem zde 7 obcí v Jihočeském kraji, kde jsem se prostřednictvím informačního zákona dotázal na implementaci obecného nařízení. Mé dotazy směřovaly hlavně na finanční a administrativní náročnost při implementaci obecného nařízení, v této kapitole chci zhodnotit náročnost implementace z pohledu správců, kteří museli upravit i zpracovatelské smlouvy k účinnosti nařízení GDPR.

Dále se chci zaměřit na revizi zpracovatelských smluv, zda právě správci byli nuceni vynaložit větší finanční prostředky a zda spolupráce správců a zpracovatelů byla v pořádku, také chci v této kapitole zhodnotit úpravu zpracovatelských smluv a možnost aplikace zpracovatelských smluv s externími subjekty.

Ve čtvrté kapitole se zaměřím na institut pověřence pro ochranu osobních údajů. Pověřenec pro ochranu osobních údajů je v českém právním řádu novinkou, chci se tedy obecně zaměřit na důvody zavedení tohoto institutu a pak zhodnotit potřebnost pověřence u orgánů veřejné moci. Zda je opravdu nutné, aby i malý správce osobních údajů, který má postavení orgánu veřejné moci, byl nucen jmenovat pověřence pro ochranu osobních údajů. Předposledním bodem u pověřence, který chci zjistit, je kolize norem a případná použitelnost správního řádu v žádostech od subjektu údajů, které budou podléhat GDPR. Tento bod záměrně zařazuji do kapitoly pověřence, protože pověřenec pro ochranu osobních údajů bude stěžejní orgán v případě vyřizování takové žádosti. V poslední podkapitole týkající se pověřence zhodnotím, jak je naplňován kontakt se subjekty údajů a jak pověřenec spolupracuje se správci osobních údajů.

V poslední kapitole se chci zaměřit na předávání osobních údajů do zahraničí. Popsat jednotlivé procesy po účinnosti GDPR a případně zhodnotit, zda tato úprava by nevyžadovala nějaké změny.

2 Obecně nařízení GDPR

2.1 Předchozí právní úprava v ČR

V 80. a 90. letech minulého století se technologie posouvaly mílovými kroky dopředu, v souvislosti s rozvojem technologií (v IT, dopravě) nastala potřeba v Evropě alespoň nějakým způsobem upravit pravidla pro zpracování, předávání a jiné operace s osobními údaji, tím nakonec byla přijata směrnice č. 95/46/ES.[1] To však neznamená, že by ochrana osobních údajů nebyla vůbec upravena před přijetím této směrnice na vnitrostátní úrovni. První předpis, který se zabýval ochranou osobních údajů, byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Zajímavé může být, že tento zákon byl přijat dříve než Listina základních práv a svobod, která stanoví nedotknutelnost soukromí.[2] Právě i s lidskými právy souvisí ochrana osobních údajů. V historii byly osobní údaje zneužívány a využívány k účelu potlačování lidských práv, zejm. v druhé světové válce byly osobní údaje, jako je třeba národnost či barva kůže, využívány k genocidě Židů, lidí s jinou pletí apod., to je také jedním z důvodů ochrany.[3]

Ochrana osobních údajů je silně spjata s právem EU. Na úrovni práva EU je právo na soukromí a ochranu osobních údajů chráněno primárním i sekundárním právem. Sekundárním právem byla ochrana zajištěna zejména již výše zmíněnou směrnicí, ta posléze byla implementována zákonem o ochraně osobních údajů[4]. Ochrana osobních údajů byla, je a bude upravena různými právními předpisy různé právní síly, počínaje od ústavního práva a evropského práva, kde Listina základních práv a svobod Evropské unie zakotvuje ochranu soukromí, [5] až po např. trestní předpisy či prováděcí vyhlášky. Do roku 2000 Česká republika neměla zákon, který by řešil ochranu osobních údajů komplexně. Tento zákon přišel až v roce 2000. Jedním z nedůležitějších aspektů tohoto zákona bylo zřízení Úřadu pro ochranu osobních údajů.[6] Vhodné je také zmínit, že soukromoprávní ochranu zajišťuje občanský zákoník, taková ochrana se pohybuje v jiném režimu než GDPR, je zde tzv. dvojkolejnost

---

[1] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018. 16–17 s.

[2] Tamtéž, s. 18.

[3] MELOTÍKOVÁ, Petra. In SLÁDEČEK, Vladimír, POUPEROVÁ, Olga. *Správní právo: zvláštní část (vybrané kapitoly)*. 2. Vydání. Praha: Leges, 2014. 132–133 s.

[4] NEUWIRT, Karel. *Ochrana osobních údajů a vstup do EU.* [online]. uoou.cz, 2003 [cit. 30. října 2018]. Dostupné na: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=8087>.

[5] Listina základních práv Evropské unie, 14. 12. 2007, Úřední věstník Evropské unie, C 303/1.

[6] *Historie úřadu pro ochranu osobních údajů*. [online]. uoou.cz, 2016. [cit. 25. Října 2018]. Dostupné na: <https://www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061/p1=1061>.

právní ochrany, jednotlivé úpravy se ale doplňují a naplňují tak svou funkci.[7] V rámci soukromého práva má dvě roviny:

a) Pozitivní – své osobnostní právo může člověk vykonávat sám podle sebe (tedy sám rozhodne, jestli se např. nechá vyfotit nebo ne).
b) Negativní – každému může zakázat, aby neoprávněně do mého soukromí zasáhl.[8]

2.2 Důvody přijetí nařízení na úrovni EU

V určité míře právo ochrany osobních údajů již bylo harmonizováno a to právě na základě směrnice č. 95/46/ES. Už obecným problémem je, že implementace takto závažného právního odvětví byla provedena právě směrnicí. Směrnice je právní akt Evropské unie, kde se vyžaduje ingerence a zásah státu v přijetí vnitrostátní legislativy.[9] Přijetí vnitrostátní legislativy na základě směrnice, ale bohužel nezabránilo roztříštěnosti v provádění ochrany osobních údajů v celé Evropské unii. Tyto rozdíly mohly vést k právní nejistotě a pocitu veřejnosti, že v souvislosti s ochranou osobních údajů fyzických osob existují velká rizika při předávání údajů fyzických osob.[10]

Hlavním důvodem přijetí je tedy unifikace ve formě nařízení, tedy odlišného právního aktu od směrnice. Nařízení je také právním aktem EU, ale pro úplnost této práce zde uvádím, že nařízení je právní akt, který je „*bezprostředně použitelný v každém členském státě ze své podstaty způsobilý mít přímý účinek, a to jak vertikální, tak i horizontální*“.[11] Horizontálním účinkem se rozumí, že fyzická nebo právnická osoba se může dovolat unijního práva mezi sebou, vertikálním účinkem se rozumí, že jednotlivec se může dovolat vymáhání předpisu vůči členskému státu[12]. K přímému účinku se mimochodem také vyjádřil SDEU, kde první judikatura ohledně přímého účinku byla v rozsudku 9/70 Grad, kde se SDEU vymezil, že společenství EU je komunitou, která je schopná zakládat práva pro jednotlivce a tím pádem nařízení má přímý účinek[13]. Nařízení je tedy přímo použitelné a transpozice není nutná, členské státy ani nemůžou přijmout obsah nařízení do svých vnitrostátních předpisů, můžou

[7] DOLEŽAL, Adam, DOLEŽAL, Tomáš. In MELZER, Filip a kol. *Občanský zákoník – velký komentář.* Svazek 1 § 1–117. Praha: Leges, 2013, s. 508.

[8] Tamtéž, s. 504.

[9] ŠIŠKOVÁ, Naděžda, STEHLÍK, Václav. *Evropské právo 1 - ústavní základy Evropské unie*. Praha: Linde, 2007, 126 s.

[10] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů*. Praktický komentář. Praha: Wolters Kluwer, 2017, s. 3.

[11] ŠIŠKOVÁ, Naděžda, STEHLÍK, Václav. *Evropské právo 1 - ústavní základy Evropské unie*. Praha: Linde, 2007, 122 s.

[12] Tamtéž.

[13] Rozsudek Evropského soudního dvora ze dne 6. října 1970, *Grad v. Finanzamt Traunstein,* 9/70, bod 9, 10.

jen přijmout pravidla k aplikaci nařízení.[14] Toto je přesně případ GDPR, v průběhu tvorby této práce je adaptační zákon k GDPR v legislativním procesu a probíhá diskuze nad jednotlivými ustanoveními tohoto zákona.

2.3 GDPR a nejdůležitější právní dopady

V zásadě, abychom stanovili nejdůležitější dopady, musíme si rozebrat hlavní pojmy, které přináší obecné nařízení o ochraně osobních údajů a z části uvést komparaci se současným stavem. V hlavní rovině si musíme stanovit, co vlastně je osobní údaj. „*Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.*“[15] Někdy je opravdu složité identifikovat, co lze za osobní údaj považovat, případně zařadit do zvláštní kategorie osobních údajů, což jsou „*takové osobní údaje, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby. Za zvláštní kategorii údajů jsou považovány i genetické a biometrické údaje, které jsou zpracovávány za účelem jedinečné identifikace fyzické osoby“*[16].

V této souvislosti právě považuji za vhodné zmínit jeden rozsudek SDEU ohledně IP adresy. Rozsudek je důkazem, že i přes definici, někdy nemusí být jasné, co přesně osobní údaj je, a co není, tedy rozlišení nemusí být vůbec snadné. Patrick Breyer, německý politik za Piratenpartei Deutschland, obdoba České Pirátské strany, napadal u německých správních soudů, že zaznamenávají a uchovávají jeho dynamické IP adresy. V první instanci byla žaloba zamítnuta, v druhé instanci soud částečně verdikt změnil a uvedl, že by Německo po skončení připojení nemělo uchovávat IP adresu ve spojení s datem otevření internetové stránky (zvlášť pokud uživatel odhalí svou totožnost – např. přihlášením do mailové adresy), v jiném případě se soud domníval, že by uchování bylo v pořádku.[17] Když se případ dostal ke Spolkovému soudnímu dvoru, ten řízení přerušil a dal předběžnou otázku, zda článek 2 písm. a) již zrušené směrnice o ochraně osobních údajů, lze vykládat tak, že dynamická IP adresa, kterou

[14] TOMÁŠEK, Michal, TÝČ, Vladimír, MALENOVSKÝ, Jiří. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017, str. 109

[15] Čl. 4 odst. 1 GDPR.

[16] Čl. 9 odst. 1 GDPR.

[17] Rozsudek SDEU ze dne 19. října 2016, ve věci C-582-14, Patrick Breyer v Bundesrepublik Deutschland, bod 49.

poskytovatel mediálních online služeb uchovává v souvislosti s přístupem uživatele na veřejně přístupnou internetovou stránku lze považovat za osobní údaj.

K této předběžné otázce se SDEU vyjádřil kladně.[18] SDEU se také zabýval problematikou dynamických IP adres, u dynamické adresy je podstatně složitější dospět k určení konkrétního jednotlivce, statické IP adresy představují neměnný údaj a zařízení je možné identifikovat prakticky kdykoliv. Dynamická IP adresa je přidělována na základě komunikace zařízení s poskytovatelem připojení, samotná dynamická adresa, bez dalších údajů neodhaluje totožnost fyzické osoby, při rozhodování ale SDEU přistoupil k použití relativního kritéria. Neřekl tedy, že v jakémkoliv případě bude IP adresa osobním údajem, ale pouze v případě, kdy je člověk identifikován, případně identifikovatelný. Toto rozhodnutí vyvolalo velkou diskuzi v oblasti ochrany osobních údajů, včetně ochrany osobních údajů v digitálním světě.[19]

Rozsudek se týkal ještě bývalé úpravy a definice v čl. 4 odst. 1 GDPR neříká, že IP adresa bude vždy osobním údajem, ale dle mého názoru judikatura není překonaná a vymezení pojmu osobní údaj se za pomoci judikatury bude více rozšiřovat. GDPR z hlediska českého právního řádu není revolucí, ale bude mít největší dopad na obecnou regulaci ochrany osobních údajů, protože balíček, který je v současné době předložen v Poslanecké sněmovně se netýká jen zrušení zákona o ochraně osobních údajů, ale dalších předpisů různého právního odvětví, (např. zákon 106/1999 Sb., o svobodném přístupu k informacím, trestní řád).[20] „Novinky“ v oblasti práva, kterých se GDPR týká, jsou vyznačeny v důvodové zprávě tohoto zákona, hlavními jsou např. nová a rozšířená práva subjektu údajů, posílení ochrany dětí a možná nejvíc zmiňované téma v médiích, povinnost jmenovat pověřence pro ochranu osobních údajů.[21]

[18] Tamtéž.

[19] NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 26. října 2018]. Dostupné na: <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.

[20] *Důvodová zpráva k návrhu zákona o zpracování osobních údajů* [online]. Úřad vlády České republiky, 2018 [cit. 23. listopadu 2018]. Dostupné na <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

[21] Tamtéž.

3 Postavení správce a zpracovatele ve vzájemných souvislostech

3.1 Správce osobních údajů a jeho (ne)přiměřené povinnosti

3.1.1 Definice správce a členění jeho povinností

Správcem osobních údajů je prakticky kdokoliv, může to být právnická i fyzická osoba, který/á určuje účely a prostředky zpracování osobních údajů. V našem konkrétním případě půjde o obce. Konkrétně obce ve své činnosti pracují s řadou informací a patří do kategorie jedněch z největších správců osobních údajů.[22] V rámci povinností, které správce má, je můžeme rozdělit do dvou následujících kategorií. První kategorií jsou povinnosti, které má každý správce, ale v druhé kategorii jsou povinnosti, které se netýkají všech správců.

1. Povinnosti, které má úplně každý správce,
   a) aplikovat záměrnou a standardní ochranu osobních údajů,
   b) zjistit, zda, je nutné provést posouzení vlivu na ochranu osobních údajů a provádět předchozí konzultace,
   c) ohlašovat případy porušení ochrany osobních údajů,[23]
2. Povinnosti, které mají jen někteří správci,
   a) jmenovat pověřence pro ochranu osobních údajů,[24]
   b) vést záznamy o činnostech zpracování,[25]

3.1.2 Povinnosti, které má každý správce

Co se týká výše uvedených povinnosti, největším problémem v praxi při dodržování ochrany osobních údajů může být jednotlivá kolize hodnot. Konkrétně tím největším problémem v rámci obecní činnosti bude kolize s jedním z důležitých principů správního práva, a to je princip transparentnosti.[26] Jde zároveň o stěžejní princip, to zároveň i z hlediska efektivity, protože skýtá všeobecnou kontrolu věcí veřejných[27], další kolizí, která v současné době již problematická je, je právo na informace a přístup k nim. To souvisí i s novelou

[22] BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 2. vyd. Praha: Linde, 2001, s. 1.

[23] ŠKORNIČKOVÁ, Eva. *Správce osobních údajů.* [online]. gdpr.cz, 2018 [cit. 23. listopadu 2018]. Dostupné na: <https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/>.

[24] Čl. 37 a násl. GDPR.

[25] Čl. 30 a násl. GDPR.

[26] HENDRYCH, Dušan a kol. *Správní právo. Obecná část.* 4. Vydání, Praha: C. H. Beck, 2001, s. 62.

[27] KOLMAN, Petr, *Úvahy o veřejném právu*. Praha: Leges, 2014, s. 9

zákona o svobodném přístupu k informacím, kde bude docházet ke kolizi ochrany soukromí a práva na informace, to z toho důvodu, že jsou to obě ústavně garantovaná práva.[28]

Pokud ale půjdeme k rozboru jednotlivých povinností následovně, u té první zjistíme, že zabezpečení osobních údajů musí být k povaze, kontextu a účelům zpracování a k různě pravděpodobným rizikům pro práva a svobody fyzických osob. Takovým rizikům se musí předcházet, a to tím, že se zavedou vhodná, technická a organizační opatření[29]. Organizačně technická opatření nejsou v nařízení, ani nikde jinde definována, jejich definice by dle mého názoru byla kontraproduktivní, protože každý správce bude potřebovat zabezpečit osobní údaje trochu jiným způsobem (např. pojišťovna, která má silně automatizované zpracování, bude zajišťovat bezpečnost trochu jiným způsobem než malá obec, která má minimum informačních systémů).

Nicméně nejsou ani definována přesně rizika, ale recitál k nařízení GDPR uvádí, co lze podřadit pod jednotlivá rizika. Jde o rizika, která by mohla vést k hmotné i nehmotné újmě kvůli diskriminaci, pověsti.[30] V tomto případě si troufám tvrdit, že recitál navazuje na rozsudek SDEU, kdy španělský občan žádal o smazání svých osobních údajů, protože při hledání jeho jména byla nalezena starší historie v souvislosti s dražbou nemovitosti a jeho dluhem na sociálním zabezpečení. Prvně španělský občan nárokoval vymazání osobních údajů z webové stránky společnosti (La Vengurdia) a v druhém nároku žádal, aby tyto údaje byly buď skryty, nebo smazány společností Google Spain, potažmo Google Inc., nicméně SDEU dospěl k závěru, že právo být zapomenut v tomto případě má být uplatněno.[31]

Dle mého názoru recitál se snaží předejít takovým případným potížím a uvádí, co přesně by mohla znamenat rizika pro práva a svobody. GDPR vychází z přístupu založeném na riziku. Domnívám se, že je to správný a logický přístup, a to už z jednoho zmíněného důvodu: každý správce bude muset řešit formu zabezpečení odlišnými způsoby (např. zdravotnické zařízení rozhodně bude muset mít IT bezpečnost mnohonásobně více vrstvenou než např. příspěvková organizace města/obce, která má ke svému účelu pouze jména a příjmení). Tedy musíme zkoumat, jaké riziko hrozí, a podle toho by osobní údaje měly být zabezpečeny.

GDPR uvádí, že vhodné zabezpečení se má posoudit vzhledem k přihlédnutím k stavu techniky, nákladům na provedení této techniky[32], jinými slovy, pokud organizace (např. právě malá obec) nemá dostatečné peníze na špičkové IT vybavení, musí vzhledem ke stavu své

[28] JELÍNKOVÁ, Jitka. *Zákon o svobodném přístupu k informacím*. Praha: Wolters Kluwer, 2017, s. 94–97.

[29] Čl. 24 odst. 1 GDPR.

[30] Čl. 72 recitálu GDPR.

[31] Soudní dvůr: Rozsudek ze dne 13. května 2014, Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12, bod 14, 15.

[32] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 96–97.

techniky podniknout taková opatření, aby zabránila úniku dat (tedy nemusí kupovat drahé šifrovací programy, případně platit za extra zabezpečený cloud na zabezpečeném serveru, ale stačí neplacené šifrování např. v souboru rar)[33].

3.1.3 Povinnosti ve spojení se šifrováním a pseudonymizací

GDPR obecně tedy zmiňuje tyto formy zabezpečení např. pseudonymizací a šifrováním. Pseudonymizace je známý fakt, který byl používán např. univerzitami (místo zveřejnění jména a příjmení studenta). Šifrování obecně zní už jako něco záhadného, případně moc IT odborného. Není tomu tak. Šifruje se pomocí tajného klíče, důležité je, aby tento klíč opravdu zůstal tajný[34], stačí např. pouze pomocí bitlockeru zaheslovat flash disk či externí disk.

V rámci tohoto kontextu musím zmínit, že pseudonymizace ani **šifrování nejsou povinnými bezpečnostními opatřeními.** Vzhledem k velkému povyku v médiích, kde bylo ohledně GDPR zmíněno mnoho nepravd a mystifikací, jedním z nich byla právě povinnost mít šifrované zařízení. Naštěstí díky osvětě Úřadu pro ochranu osobních údajů se velkou část mýtů podařilo dementovat z internetového světa. O šifrování již bylo zmíněno pár vět výše. Šifrování je vhodná forma bezpečnostního opatření zejm., pro tzv. „přenosové disky“ typu flash, externí harddisk, šifrováním se zmenšuje šance, že by se někdo neoprávněný mohl dostat k datům, ke kterým by za normálních okolností, neměl mít přístup. Jak již bylo zmíněno výše, forma šifrování může být různá, v dnešní době rozvoje IT technologií se poměrně jednoduše dají použít aplikace k šifrování, které nabízí sám Microsoft v rámci operačního programu Windows (Bitlocker). V případě nejistoty zabezpečení je vhodné použít tzv. penetrační test. Jedná se o metodu etického hackingu, kdy expert v oblasti IT bezpečnosti záměrně zkouší prolomit zabezpečení.[35]

Pseudonymizace je operace ne příliš náročná, stačí např. pouze přidělit jednotlivým žákům školy číslo a pouze tato čísla zveřejnit např. na webových stránkách školy, číslo žáka je pak dohledatelné v jeho osobním spise, případně v kanceláři ředitele školy. Na webu však je dohledatelné jen rozhodnutí o ne/přijetí a číslo, pod kterým je žák „utajen“. Např. nesprávný postup mají některé univerzity, které nepostupují dle platné a účinné legislativy, zveřejňují jména a příjmení studentů i den jejich státní závěrečné zkoušky. Účel zpracování zde jednoznačně byl překročen, za pravdu mi dává i stanovisko ÚOOÚ[36]. Přesně pro tento

[33] Uvádím pouze jako příklad, nelze vždy konkrétně říci, že tato volba je vhodná.

[34] NEZMAR, Luděk. *GDPR Praktický průvodce implementací*. Praha: Grada Publishing, 2017, s. 245.

[35] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 97.

[36] *Zveřejňování osobních údajů studentů* [online]. uoou.cz, 18. dubna 2013 [cit. 25. listopadu 2018]. Dostupné na <https://www.uoou.cz/zverejnovani-osobnich-udaju-studentu/d-1756>.

případ je vhodné použít pseudonymizaci osobních údajů (nikoliv osobním číslem studenta, které je dohledatelné i pro jiné studenty ve STAGu nebo jiném informačním systému univerzity. Taková praxe opět byla na některých univerzitách, v současné době tento nedostatek již byl u některých napraven).

Další povinností správce je vůbec zjistit, zda je potřebné, aby provedl posouzení vlivu na ochranu osobních údajů. Není tedy třeba provádět **vždy** samotné posouzení vlivu na ochranu osobních údajů, ale správce musí vyvinout takovou aktivitu, aby zjistil, zda je nutné posouzení vůbec provádět. Důležité je zmínit, že posouzení vlivu není třeba pro zpracování, které probíhalo před účinnosti GDPR (s výjimkou, kdy ve zpracování dojde ke změně, to je opět na posouzení správce).[37] Skupina WP 29 výborně graficky zpracovala graf, kdy je posouzení vlivu na ochranu osobních údajů povinné a kdy se obejde bez posouzení. Jak je vidět z grafu níže[38], posouzení vlivu na ochranu osobních údajů bude povinné zejm., pokud určitý druh zpracování bude mít za následek vysoké riziko[39]. Co je vysoké riziko, není přesně nikde definováno, vždy se taková skutečnost bude muset posuzovat individuálně. Pracovní skupina WP29 ale zpracovala vodítka, která můžou být nápomocna k určení, zda o takové zpracování půjde (jde např. hodnocení zahrnující profilování, propojování různých databází atd.)[40] Jinými slovy, správce v každém případě bude muset posoudit, zda nějaké zpracování vykazuje vysokou míru rizika pro práva a svobody subjektu údajů. V případě, že dospěje k tomu, že ano, dalším krokem bude zhodnocení, jestli zpracování nespadá pod čl. 35 odst. 5 nebo čl. 35 odst. 10, tedy v prvním případě případ, kdy Úřad zveřejní seznam zpracování, u kterých není nutné posouzení vlivu na ochranu osobních údajů[41], v druhém případě by šlo o zpracování, které má základ v právu EU a posouzení vlivu již bylo učiněno, a tedy není nutné. Tato povinnost by měla být zpřesněna v rámci adaptačního zákona.[42] V ostatních případech, kdy správce dospěje k posouzení vlivu, bude pro něj povinné a v určitých případech bude správce mít dokonce povinnost konzultovat zpracování s dozorovým úřadem, jak značí graf.

---

[37] ČERNÝ, Jiří. In PATTYNOVÁ, Jan a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018, s. 270.

[38] Pokyny Pracovní skupiny 29 „*pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko*“ pro účely nařízení 2016/679 ze dne 4. dubna 2017, aktualizované stanovisko 4. října 2017, s. 8.

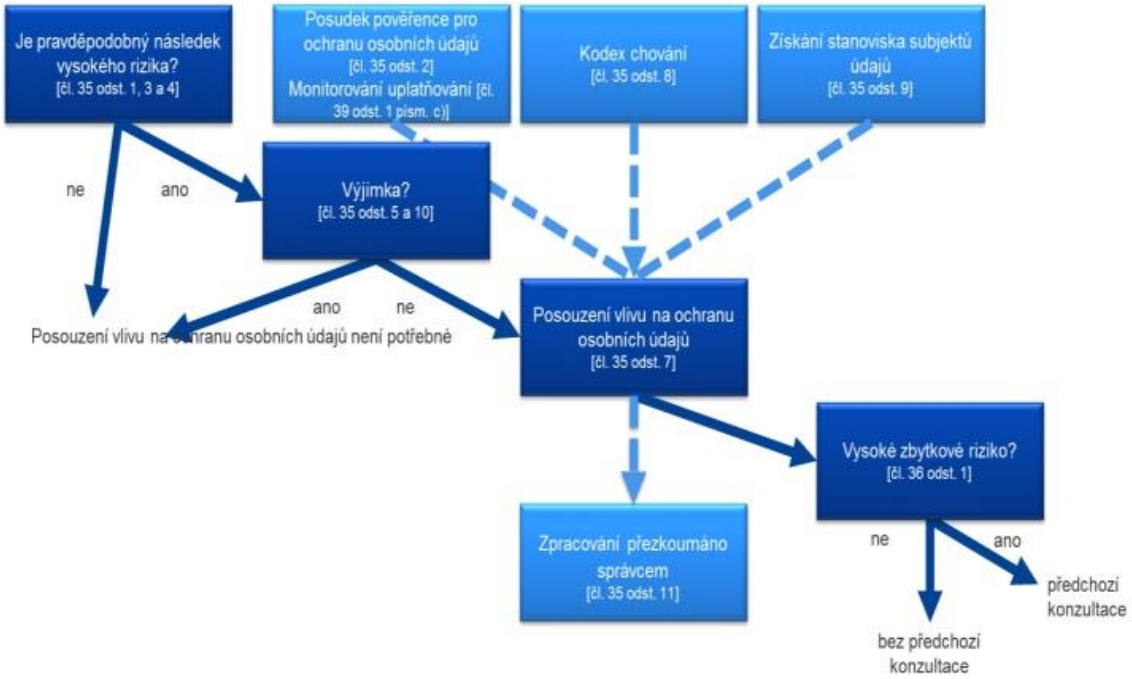
[39] Co je vysoké riziko není přesně určeno, vždy se taková věc bude muset posuzovat individuálně, určitý návod ale poskytuje recitál obecného nařízení např. v čl. 85.

[40] Pokyny Pracovní skupiny 29 „*pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko*“ pro účely nařízení 2016/679 ze dne 4. dubna 2017, aktualizované stanovisko 4. října 2017, s. 10.

[41] Tamtéž, s. 8.

[42] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 125.

Graf 1: Základní principy k posouzení vlivu na ochranu osobních údajů



Zdroj: [43]

Poslední povinností, která platí pro všechny správce je hlášení bezpečnostních incidentů. Obecně můžeme hlášení bezpečnostních incidentů rozdělit tímto způsobem:

a) dle článku 33, kdy jde o oznamování případů porušení zabezpečení osobních údajů dozorovému úřadu.[44]

b) dle článku 34, kdy jde o oznamování případů porušení zabezpečení osobních údajů subjektu údajů.[45]

Povinnost hlásit porušení zabezpečení osobních údajů dozorovému úřadu nevzniká vždy, opět jde zde přístup založený na riziku. Tedy pokud je nepravděpodobné, že by tento postup měl následek za riziko pro práva a svobody fyzických osob[46], správce není povinen hlásit porušení zabezpečení osobních údajů. Otázkou však zůstává, kde je hranice mezi „nepravděpodobným a pravděpodobným" rizikem. Jako příklad ale můžeme uvést jednoduchou věc, obecní úředník má na svém zašifrovaném externím disku pseudonymizované osobní údaje jednotlivců, kteří v daný rok nezaplatili místní poplatek za psa, úředník tedy ví, že i v případě prolomení disku – (zde bude vždy záležet na kvalitě šifrování) se v případě ztráty nikdo nedozví, kdo dluží v obci místní poplatek, protože formu

[43]Pokyny Pracovní skupiny 29 „*pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko*" pro účely nařízení 2016/679 ze dne 4. dubna 2017, aktualizované stanovisko 4. října 2017, s. 8

[44] Čl. 33 odst. 1 GDPR.

[45] Čl. 34 odst. 1 GDPR.

[46] Čl. 33 a násl. GDPR.

pseudonymizace zná pouze úředník. Domnívám se, že to je přesně případ, který **nevyžaduje** ohlášení dozorovému úřadu. V případě pozdějšího prolomení klíče, by však bylo nutné porušení zabezpečení ohlásit. To však neznamená, že by správce neměl vůbec žádné povinnosti, správce musí i takové porušení řádně zadokumentovat a uvést skutečnosti, které se týkají porušení zabezpečení, včetně nápravy.[47] Dle mého názoru je tato povinnost logická, správce by poté jednoduše mohl zlehčovat význam bezpečnostních opatření, případně by mohl úmyslně ztratit různá data ve vlastním zájmu (např. ukradení know – how firmy odcházejícím zaměstnancem).

V ostatních případech vzniká povinnost takovou skutečnost hlásit dozorovému úřad (pokud se zároveň nenaplní i podmínky pro hlášení subjektům údajů.) Tím se dostáváme do další povinnosti správce, který v případě, kdy hrozí vysoké riziko pro práva a svobody fyzických osob s určitými výjimkami (pokud správce provedl organizační a technická zabezpečení, která činí údaje nesrozumitelnými, případně přijal taková opatření, že se vysoké riziko neprojeví nebo by vyžadovalo neúměrné úsilí), pokud není naplněna tato výjimka, toto porušení zabezpečení musí být ohlášeno, včetně hlášení subjektům údajů. Ukázkovým příkladem může být jakákoliv nemocnice. Nemocnice vede poměrně citlivé údaje o svých klientech (pacientech), záznamy v nemocnici nebudou dostupné po dobu 30 hodin v důsledku útoku na informační systémy nemocnice. V takovém případě vzniká povinnost hlásit vše dozorovému úřadu i dotčeným subjektům údajů, a to vzhledem k vysokému riziku pro pacientova zdraví a soukromí[48]. Toto jsou povinnosti, které má každý správce.

3.1.4 Povinnosti, které nemá každý správce

Další povinnosti, které nemá každý správce, jsou dvě, případné jmenování pověřence pro ochranu osobních údajů a vedení záznamů o činnostech. Povinnost jmenovat pověřence a další povinnosti, které jsou spjaté s tímto institutem, jsou rozebrány v samostatné kapitole. Záznamy o činnostech ale jsou poměrně diskutovaným tématem, povinnost vést záznamy o činnostech nedopadá na všechny správce, v článku 30 je uvedena výjimka, která je v čl. 30. odst. 5. Problematickým zde je slovo příležitostné. GDPR nikde vyloženě nedefinuje, co je příležitostné zpracování osobních údajů. V praxi a literatuře na to kolují dva názory, jeden se přiklání ke gramatickému výkladu, kdy se tvrdí, že příležitostné zpracování je prakticky jakékoli zpracování, ke kterému nedochází soustavně.[49]

[47] Čl. 33 odst. 5 GDPR.

[48] JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018 str. 73.

[49] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 286.

Druhý názor je diametrálně odlišný, a to, že o příležitostné zpracování nejde, jestli je pevně spojeno s hlavní činností správce (např. provozovatel datového centra těžko bude tvrdit, že zpracování osobních údajů souvisí jen příležitostně).[50] Já se osobně přikláním k druhému vyjádřenému názoru, protože v případě aplikace prvního názoru v praxi by ustanovení bylo neúčinné. Např. každá organizace ve veřejné správě i v soukromém sektoru vede mzdové účetnictví, kde se zaznamenává plat nebo mzda jednotlivých zaměstnanců, pokud tedy dochází k výplatě každý měsíc, v tomto případě by se nikdy nemohlo jednat o příležitostné zpracování. Smysl vidím právě v druhém názoru na toto ustanovení, protože pokud malá organizace např. firma, která provozuje zemědělskou činnost, má dva zaměstnance na plný úvazek a dále jen brigádníky, kteří nastupují na sezónní práce, pro takovou firmu by bylo neúčelné, aby vedli záznamy o činnostech, protože hlavní činnost správce není činnost s osobními údaji, případně vedení účetnictví, ale pokus o generování zisku v oblasti zemědělství. Mzdové účetnictví není spojeno s hlavní činností správce, ale jako vedlejší podpůrná činnost ke splnění právních předpisů a smluvních vztahů (daňové odvody, výplata). Nicméně, v neformální komunikaci na ÚOOU během konzultací pro pověřence, kterých jsem se účastnil v říjnu 2018, převládá názor, který v této práci neprezentuji (mzdové účetnictví se nepovažuje za příležitostné zpracování). I samotné ÚOOU doporučuje vyplnit záznamy o činnostech pro organizace, které si nejsou jisté, jestli do výjimky spadají, tento přístup považuji za nesprávný.[51]

3.2 Postavení správce a zpracovatele v rámci obecní činnosti

V rámci činností, které obec jako organizace a správce provádí, není v silách jednotlivých obcí veškerou činnost pokrýt samostatně. Z tohoto důvodu obce různě najímají např. IT firmy za účelem vytvoření bezpečného kybernetického prostředí. Nemusí jít samozřejmě jen o informační technologie, ale může jít i zpracování mezd nebo obecného účetnictví. Tedy správce najímá externí dodavatele, kteří se starají nebo vylepšují IT systém, případně zpracovávají jinou agendu obce (např. právě již zmíněné mzdy). V souvislosti s povinnostmi v článku 28 nařízení, který stanoví, že správce musí vybrat takového zpracovatele, který zajistí dostatečnou úroveň ochrany osobních údajů, včetně dostatečné ochrany práv soukromí člověka. Na základě této skutečnosti jsem oslovil některé subjekty dle zákona č. 106/1999

[50] KRÁL, Štefan. In PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018, s. 249.

[51] *Základní příručka k GDPR* [online]. uoou.cz, 2018 [cit. 30. října 2018]. Dostupné na <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744>.

Sb., o svobodném přístupu k informacím a zeptal se zejm., jak problematické bylo uzavírání smluv se zpracovateli.

Oslovil jsem tyto subjekty:

a) Obec Chroboly,
b) Město Volyně,
c) Obec Kvilda,
d) Obec Lenora,
e) Město Písek,
f) Obec Horní Vltavice,
g) Městys Strážný.

V příloze uvádím jednotlivé odpovědi starostek/starostů na mou žádost. Obecně lze říci, že ze žádostí vyplývá pesimistický přístup představitelů obcí vůči obecnému nařízení o ochraně osobních údajů fyzických osob. Dovolím si tvrdit na základě odpovědí, že jednotlivým představitelům přijdou povinnosti v nařízení nadbytečné, např. obec Chroboly poukázala na dobře zpracovaný zákon o ochraně osobních údajů. Jejich odpovědi nelze brát jako vědecké či relevantní v rámci statistiky, jelikož častou odpovědí byla nevěcná kritika nařízení a vágní odpověď, viz příloha. Mé dotazy směřovaly zejm., na zpracovatelské smlouvy, které obce musely uzavřít s těmito subjekty. V rámci zpracovatelských smluv lze předpokládat, že jejich úprava může být poměrně finančně náročná a ovlivní správce i zpracovatele. Postavení správce a zpracovatele a uzavření zpracovatelské smlouvy jsou v některých případech nevyhnutelné, otázkou již jen zůstává, jaká cenová relace a jaké smluvní podmínky budou nastaveny v rámci zpracovatelských smluv. Z tohoto důvodu jsem vybral obce, které mají pověřený obecní úřad (Volyně) i obec, která je obcí s rozšířenou působností (město Písek), zbytek obcí jsou obce tzv. „prvního typu“.[52] Např. jak již bylo zmíněno, není v síle obcí s rozpočtem kolem 10 miliónů ročně zajistit IT pracovníka a IT systémy, které by odpovídaly vícevrstvené kyberbezpečnosti.

Osobně mě překvapilo, že všechny oslovené obce zmínily, že se zpracovateli žádný problém nebyl a že byli nakloněni spolupráci, pouze město Písek a Volyně uvedla drobné výtky. Město Písek uvedlo, že implementace vyžadovala menší úpravy ve smlouvách, nikoliv však zásah do obecního rozpočtu. Jediné město, které otevřeně přiznalo zvýšenou míru nákladů na chod úřadu, bylo město Volyně, a to modernizací IT vybavení z dotace, vylepšení a zabezpečení sítě a zálohování informačních systémů. Zároveň uvedlo zvýšené náklady na

[52] Zákon č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností.

právní služby, které se pohybují v rozmezí cca 30 000 Kč.[53] Nejdůležitější faktor v uzavírání smlouvy mezi správcem a zpracovatelem je fakt, že pokud správce určí svého zpracovatele, pořád je správce ten, který má obecnou odpovědnost za soulad se zpracováním a sám správce je ten subjekt, který má zároveň i odpovědnost za uzavření jakéhokoliv právního aktu se zpracovatelem. Obecnou odpovědnost správce nikdy na zpracovatele nelze přenést.[54] Pokud by došlo k porušení zabezpečení v důsledku chyby zpracovatele a bylo to prokázáno, bude odpovědný zpracovatel, ale za své samostatné jednání, nikoliv za chyby správce, uplatňuje se takový výklad, že odpovědnost správce by v tomto případě měla být vyloučena[55]. Osobně se domnívám, že pokud by tedy došlo k chybě v důsledku zpracovatele, odpovědnost by v určitých případech (podotýkám, že ne vždy)[56] měl nést i správce (solidárně), protože právě správce zpracovatele vybral. Vhodné je ale zmínit, že vždy bude záležet na smluvním vztahu mezi správcem a zpracovatelem[57] a konkrétní obecné řešení předem tedy nelze stanovit.

3.3 Úprava zpracovatelských smluv a souvisejících činností z hlediska aplikace u činnosti obcí ve světle efektivity veřejné správy

Nejdůležitější zásady, které se promítají ve vztahu správce a zpracovatele jsou zásada minimalizace údajů, zásada odpovědnosti a zásada účelového omezení. Zásada minimalizace údajů je vyjádřena v čl. 5 nařízení GDPR, který stanoví, že osobní údaje musí být přiměřené a také omezené na účel zpracování. To v praxi bude znamenat, že správce musí velmi důkladně zvážit, jaké osobní údaje bude zpracovávat. To také vždy bude záležet na konkrétní situaci. Druhá zásada je zásada odpovědnosti. Zásada odpovědnosti vychází z dvou predikcí, s tím, že správce odpovídá za dodržení všech povinností z GDPR, nicméně taková povinnost byla již dříve[58]. Ale GDPR také ukládá novou povinnost a tou je, že soulad musí i prokázat. Takový soulad se právě nejlépe prokáže auditem ochrany osobních údajů (označované také jako GAP analýza), v této analýze je třeba zhodnotit i současné smlouvy. Dejme tomu, že

[53] V rámci této práce jsem oslovil výše zmíněné subjekty dle zákona o svobodném přístupu k informacím, odpovědi a otázka lze najít v příloze této práce. Jelikož odpovědi byly velmi nedostačující ke kvalitnímu výzkumu, rozhodl jsem se je publikovat volnější formou v příloze. Zároveň jsem se setkal i s neochotou některých správců takové informace poskytovat, byť to nejsou informace vyňaté z informačního zákona.

[54] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 91–93.

[55] Tamtéž, s. 92–94.

[56] Vždy bude záležet na konkrétním porušení, v určitých případech se může stát, že správce poskytne nepřesné informace a v takovém důsledku zpracovatel učiní chybu (za předpokladu, že jeho smluvní povinností bylo překontrolovat řádný stav a on tak neučinil), v tomto případě se domnívám, že by to měl být přesně případ, kdy by bylo vhodné využít solidární odpovědnost

[57] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 92 - 94

[58] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

audit, nebo posouzení současného stavu se stavem, jak by to mělo vypadat dle GDPR znamená, že obec se musí zaměřit na procesy organizace, využívané osobní údaje, také se musí zaměřit na aplikaci technických a organizačních opatření zaměřených na ochranu informací. Dále bude muset vyvinout poměrně velkou administrativní činnost v revizi dokumentace (nejen smluvní) obce a jejího využívání. Právě taková analýza předpokládá zhodnocení stavu správce (obce) a jejich zpracovatelů, tedy subjektů, které jí osobní údaje zpracovávají. V rámci GAP analýzy bude potřebné, aby právě revize zpracovatelských smluv byla řádně zpracována.

Požadavky oproti směrnici jsou v GDPR trochu rozšířeny, proto je třeba vyvinout větší pozornost v jejich případné revizi. Zpracovatelská smlouva musí mít písemnou formu dle čl. 28 odst. 9, při čemž GDPR nestanoví, co písemná forma je a co písemná forma není, tedy budeme muset vycházet z pravidel NOZ, konkrétně § 562 a násl.[59]. Právní jednání v písemné formě je zachováno i v jednání, které je učiněné v elektronické formě. Lze předpokládat, že v dnešním digitálním světě bude většina komunikace prostřednictvím elektronické formy. Pod pojmem elektronické komunikace lze podřadit internet, mobilní telefon apod. K tomu, aby byla elektronická forma zachována, musí být splněny dva předpoklady:

a) Musí umožnit zachycení právního jednání – tzn., že např. lze uchovat e-mail, nebo textovou zprávu.
b) Lze identifikovat jednající osobu – to už může být v určitých směrech problematická otázka, zda bude stačit pouze jakákoli možnost určení jednající osoby (např. e-mailem – případně bude třeba přísnější forma.[60] Osobně v případě jednání, které se bude týkat zpracování osobních údajů, zastávám názor stejný jako komentářová literatura, tedy, že požadovaná důvěryhodnost ověření totožnosti by měla odpovídat riziku újmy[61], což považuji za adekvátní.

[59] HRDLIČKA, Miloslav. In LAVICKÝ, Petr. *Občanský zákoník: komentář.* Praha: C.H. Beck, 2015, s. 2025–2026.

[60] Tamtéž, s. 2025.

[61] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 185.

Nejdůležitější body revize smluv mezi správcem a zpracovatelem jsou shrnuty v následujících bodech:

I. Předmět zpracování

Ve smlouvě musí být jasně vymezeno, co je předmětem zpracování, ve zpracovatelské smlouvě nelze generálně říci, že předmětem zpracování budou všechny osobní údaje. Tedy v předmětu zpracování by měly být vymezeny jednotlivé kategorie osobních údajů[62]. Literatura uvádí, že postačí např. označení „fotografie“, v tomto případě se tak nedomnívám a myslím si, že by tato informace měla být konkretizovanější. Fotografie je sama o sobě specifický osobní údaj, který často může vyvolávat odbornou diskuzi, zda vůbec dochází ke zpracování osobních údajů, někdy totiž při fotografování již pořízený obrázek nespadne do věcné působnosti nařízení.[63]

II. Účel a doba zpracování

Osobní údaje vždy správce osobních údajů uchovává z nějakého účelu, tento účel by měl být stanoven jasně a konkrétně. Zároveň účel nesmí překračovat původní účel zpracování, to znamená, že pokud by např. obec na základě právního titulu plnění smlouvy zasílala informace ohledně dění v obci, měla by účel i právní titul, který by postačil na zákonné zpracování[64]. Pokud by, ale začala posílat marketingové nabídky za účelem získání nových zákazníků pro firmu starosty, již by byl účel překročen a tím by bylo zpracování osobních údajů nelegální.

III. Kategorie osobních údajů

O typu osobních údajů již bylo zmíněno v rámci předmětu zpracování, kategorie subjektu údajů jsou jiným typem, jde o tzv. fyzické osoby, kterých se zpracování osobních údajů dotýká (vyloženě např. zaměstnanci atd.)[65]

IV. Vázanost doloženými pokyny správce

Pokyny, kterými je zpracovatel vázán, musí být řádně doložené, tzn., že zpracovatel nemůže předat osobní údaje někomu jinému, mimo stanovené výjimky, tyto výjimky jsou buď případy, kdy to ukládá právo členského státu nebo právo EU. Je tedy nad míru vhodné, aby

---

[62] Tamtéž, s. 277.

[63] *Stanovisko č. 12/2012 aktualizace říjen 2017 K použití fotografie, obrazového a zvukového záznamu fyzické osoby*. [online]. uoou.cz 20. listopadu 2017. [cit. 26. listopadu 2018]. Dostupné na <https://www.uoou.cz/stanovisko-c-12-2012-k-pouziti-fotografie-obrazoveho-a-zvukoveho-zaznamu-fyzicke-osoby-aktualizace-rijen-2017/d-27693/p1=0>.

[64] HEJLÍK, Ladislav. *Zpracování osobních údajů v rámci služeb SMS infokanál.* [online]. uoou.cz 13. února 2018. [cit. 30. listopadu 2018]. Dostupné na <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32116>.

[65] Pro lepší pochopení termínu kategorie osobních údajů je možné využít vzorové záznamy o činnostech vydané MŠMT, případně MV ČR. Vše dostupné na oficiálních webových stránkách obou ministerstev.

správce osobních údajů dostatečně pokyny specifikoval. To, že zpracovatel komunikací se správcem či svou nabídkou na uzavření smlouvy určuje, jaké pokyny může správce ohledně zpracování udělit, neznamená, že by určoval účely zpracování (typicky účetní software pro obce), účetní firmy sice pošlou adhezní smlouvu, ale účely zpracování stejně určuje obec (správce) osobních údajů.

Hlavní je finální kontrola nad účely zpracování[66], v určitých bodech, ale vidím kritické, že v případě adhezních smluv, tedy u smluv, kde reálně jedna ze stran nemá možnost ovlivnit obsah, se správce dostává do značně nevýhodného postavení a je otázkou odborné diskuze, zda zpracovatelské smlouvy mohou sloužit jako adhezní, některá komentářová literatura uvádí, že ano[67]. Já se s tímto názorem ztotožňuji, ale poukazuji na dva problémy, které v budoucí praxi můžou vyvstat. Přímo v § 1798 NOZ je předpoklad, že v adhezních smlouvách zřejmě bude slabší strana a ta se pokusí reálně vyjednávat o obsahu základních podmínek a pokud toto ovlivnění bude vyloučeno, bude se jednat jasně o adhezní smlouvu, tedy lze předpokládat, že správce by vystupoval v postavení slabší strany vůči zpracovateli.[68] Tedy bude nucen přijmout podmínky např. slabší ochrany šifrování než by si reálně představoval. Slabší stranou by byl správce v terminologii soukromého práva, ale přesto si myslím, že podstatné vždy bude, jak případná smlouva může ovlivnit práva a svobody subjektů údajů[69].

Druhým problémem je, že mnoho činností, které lze na první pohled považovat za zpracování osobních údajů, se v konečném důsledku jako zpracování také považovat nebude (např. pouhé na nahlížení do elektronického systému externí IT společností se za zpracování ve smyslu GDPR považovat zřejmě nebude). V takovém případě nebude vyloženě nutné uzavírat zpracovatelskou smlouvu, nepůjde totiž o zpracovatele dle čl. 28 GDPR, ale osoby, které jednají z pověření správce a mají přístup k osobním údajům ve smyslu čl. 29 GDPR. Samozřejmě, že s těmito osobami se předpokládá uzavření smlouvy, která není typově zpracovatelská, ale bude obsahovat závazky týkající se zajištění bezpečnosti, mlčenlivosti, a řízení se pokyny správce. Tedy v praxi bude docházet k nadbytečnému užívání zpracovatelských smluv.

---

[66] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů*. Praktický komentář. Praha: Wolters Kluwer, 2017, s. 278.

[67] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů*. Praktický komentář. Praha: Wolters Kluwer, 2017, s. 278.

[68] PETROV, Jan. In HULMÁK, Milan. *Občanský zákoník V: závazkové právo: obecná část* (§ 1721-2054): komentář. Praha: C.H. Beck, 2014, s. 345.

[69] Princip založený na riziku

3.4 Odpovědnost správce a zpracovatele a postavení ÚOOU

Odpovědnost správce za porušení GDPR je logicky spojena s možností nějaké sankce. V rámci České republiky před účinností nařízení GDPR kolovaly velké fámy ohledně nařízení, které dokonce musel vyvracet sám ÚOOU, a to odkazem „desatero omylů“[70]. Největším omylem obecně bylo odkazováno na nařízení GDPR jako na směrnici, případně udělování pokut za volně dostupnou wi-fi[71], občas také bylo strašeno revolucí v osobních údajích u zaměstnanců[72]. Tyto sankce dle nové terminologie lze nazvat správním trestem. Správní trest je následek za spáchání přestupku, základní premisou u správního trestu je způsobení újmy.[73] Tedy obecným smyslem správního trestu je ochrana společnosti v tom, že by případná sankce měla zabránit pachateli dalšímu takovému jednání, zároveň by měla fungovat sankčně jako trest za nedodržení povinností.[74]

Pokuty lze zformovat do dvou kategorií. První kategorií je pokuta do 10 000 000 milionu EUR (případně 2 % z celkového ročního obratu), druhou kategorií do 20 000 000 (případně 4 % z celkového ročního obratu). Na první pohled se tyto pokuty můžou zdát vysoké, je třeba si ale uvědomit, že jsou to pokuty, které jsou pro všechny správce, nikoliv jen pro malé živnostníky, pro malé obce, ale také pro společnosti jako je např. Google. Právě tato společnost měla zisk jen za první čtvrtletí roku 2018 v přepočtu 195,9 miliardy Kč.[75] Současný zákon o ochraně osobních údajů uděluje pokuty až do 10 000 000 Kč[76], pro většinu fyzických osob je samozřejmě tato částka likvidační, ale pro právnickou osobu jako je Google by byla velmi nepatrnou částkou. Zároveň je také třeba vnímat ono předchozí rozdělení. Kategorie pokut jsou dány důležitostí porušené povinnosti (rozdíl bude, pokud obec ztratí záznamy o činnostech nebo použije údaje z evidence obyvatel za účelem přímého marketingu pro firmu starosty). Vždy se každá sankce bude muset posuzovat individuálně.

To však neznamená, že vždy za každé porušení musí být udělena pokuta, sankce finanční pokutou by se měly využívat jako prostředek „*ultima ratio*“[77], v zájmu ochrany osobních údajů není účelem správce likvidovat, ale zejm., naučit je řádně osobní údaje chránit. Jiná

---

[70] *Desatero omylů.* [online]. uoou.cz, 2017. [cit. 30. listopadu 2018]. Dostupné na <https://www.uoou.cz/desatero-omylu/ds-4818/p1=4818>.

[71] *Nepravdy o wi-fi*. [online]. uoou.cz, 2017. [cit. 30. listopadu 2018]. Dostupné na https://www.uoou.cz/nepravdy-o-wi-fi-v-souvislosti-s-gdpr/d-28774.

[72] CHLÁDKOVÁ, Alena. *Osobní údaje v pracovněprávních vztazích. Práce a mzda*, 2018, roč. 66 č. 5, s. 6.

[73] S tím souvisí zároveň také přístup založený na riziku.

[74] FIALA, Zdeněk a kol. *Správní právo trestní*. Praha: Leges, 2017. s. 105, 106.

[75] FIEGERMAN, Seth. *Google posts its first $100 billion year.* [online]. money.cnn.com, 1. ledna. 2018. [cit. 30. listopadu 2018]. Dostupné na:< https://money.cnn.com/2018/02/01/technology/google-earnings/index.html>.

[76] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[77] Zde pouze vyjadřuji svou představu o smyslu kontroly ve veřejné správě (v závislosti na hmotněprávním korektivu správního trestání) byť chápu, že realita úředníků může být dost odlišná.

nápravná opatření můžou být využita, když se zpracování má uvést do podoby, která odpovídá právnímu řádu v určité lhůtě, případně pouze udělit napomenutí. Těchto opatření k nápravě je více a sankce dle GDPR neznamená pouze ukládání pokut. Taková opatření jsou vyčtena v čl. 58 odst. 1 písm. a) – j) GDPR.

V českých médiích byla silně používána, troufnu si říct, mediální masáž a mediální kampaň, která měla za účel jediný cíl, a to správce osobních údajů vystrašit a vyfakturovat. Vedly se různé online marketingové kampaně, které tvrdily, jak výše pokut může být likvidační[78]. K tomu je jen třeba dodat, že takové účelové jednání byla čistá demagogie. Nejvyšší pokutu, kterou ÚOOU udělil, byla pokuta ve výši 4, 5 milionu korun, a to soukromé společnosti za nevyžádané posílání obchodních sdělení. Důvodem takové výše byl ještě navíc velký počet stížností přímo od subjektů údajů.[79] Dozorový úřad a jeho kompetence upravuje čl. 51 GDPR a následující, dosud byl dozorový úřad zřízen zákonem o ochraně osobních údajů[80], adaptační zákon nepočítá s ničím jiným, výslovně stanoví, že Úřad pro ochranu osobních údajů je Ústředním správním úřadem.[81] Samotný článek 52 stanovuje jednu z nejdůležitějších zásad, to je nezávislost dozorového úřadu. Nezávislost lze chápat ve více různých směrech, já osobně zastávám názor, který se vyskytuje v odborné literatuře. Nezávislost lze chápat v těchto třech směrech:

a) Nezávislost funkční – tedy, že ÚOOU funguje bez nějakých vnějších vlivů.
b) Nezávislost materiální – lze chápat tak, že ÚOOU má dostatek lidských a finančních kapacit, není na nikom závislý. Tato nezávislost je zakotvena v návrhu zákona o ochraně osobních údajů v § 49 odst. 2, který stanoví, že činnost ÚOOU bude hrazena ze samostatné kapitoly státního rozpočtu. Otázkou samozřejmě zůstává, jak tato kapitola bude vypadat, pokud dojde k podfinancování ÚOOU. Je logické, že nebude moci vykonávat svoje pole působnosti řádným způsobem, jestli k takové situaci dojde, to už je ale politická, nikoliv právní otázka.
c) Nezávislost personální – personální nezávislost souvisí s obsazením jednotlivých pracovníků, kteří budou mít dostatečnou kvalifikaci.[82]

[78] Kyberbezpečnost – Forbes. *Milionové pokuty za únik dat.* [online]. kyberbezpecnost.forbes.com, 2017. [cit. 30. listopadu 2018]. Dostupné na: <https://money.cnn.com/2018/02/01/technology/google-earnings/index.html>.

[79] *Tisková zpráva uoou udělil rekordní pokutu za spam*. [online]. uoou.cz, 2017. [cit. 30. Listopadu 2018]. Dostupné na: <https://www.uoou.cz/tiskova-zprava-uoou-udelil-rekordni-pokutu-za-nbsp-spam/d-23838/p1=1017>.

[80] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[81] *Důvodová zpráva k návrhu zákona o zpracování osobních údajů* [online]. Úřad vlády České republiky, 2018 [cit. 1. prosince 2018]. Dostupné na <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>

[82] PINKAVOVÁ, Adéla. In PATTYNOVÁ a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018, s. 360–363.

4 Pověřenec pro ochranu osobních údajů

4.1 Důvody zavedení institutu pověřence

Sám institut pověřence pro ochranu osobních údajů není novinkou v právním řádě v Evropě, např. v Německu byl zaveden již v 70. letech[83]. To znamená, že byl sám zaveden ještě před vznikem směrnice o ochraně osobních údajů. Další státy, které mají pověřence pro ochranu osobních údajů, jsou Nizozemsko, Francie a před účinností GDPR dokonce i Slovensko. Zároveň skupina WP29 poukazovala ve svých dřívějších stanoviscích, že pro některé podniky/úřady je vhodné jmenovat osobu, která by odpovídala, případně by byla odpovědná za agendu osobních údajů. Tím by totiž byla lépe naplněna zásada odpovědnosti.[84] K tomu je vhodné ale zmínit, že např. německý koncept ochrany osobních údajů byl jiný než český, dokud nedošlo k harmonizaci obecným nařízením o ochraně osobních údajů (GDPR). V rámci ochrany osobních údajů byla zavedena funkce pověřence, zejm. jako „strážce" osobních údajů. Dovolím si tvrdit, že v dnešní informační společnosti byl tento institut zřízen zejména proto, aby fungoval jako „ombudsman" pro subjekty údajů ještě před tím, než by nějaký určitý konflikt či problém došel do fáze soudního řízení.

Zároveň GDPR stanovuje určité povinnosti, které by určitým správcům mohly dělat potíže (např., posouzení vlivu na ochranu osobních údajů), tedy dají se předpokládat vyšší nároky při zpracování osobních údajů v některých případech. V praktické rovině se dá říci, že dalším z důvodů zavedení institutu pověřence napříč celou Evropou je zvýšená ochrana osobních údajů a zrychlený proces vyřízení případných práv od subjektu údajů. Tedy je podstatné, aby se pověřenec pro ochranu osobních údajů (případně jeho expertní tým) zapojil do veškerých záležitostí souvisejících s ochranou osobních údajů tím, že bude informován a bude do všech procesů ochrany osobních údajů zapojen včas, tím se zajistí dodržování souladu s obecným nařízením o ochraně osobních údajů. Zároveň je také důležité, aby subjekty, které mají povinnost pověřence zřídit, nebraly tuto funkci jako něco, co je přítěží pro organizaci.

[83] § 5 odst. 1. BDSG.

[84] Stanovisko Pracovní skupiny WP29– *On the principle of accountability* – č. 3/2010 ze dne 13. července 2010, s. 4

Pověřenec má být diskuzní partner a měl by splňovat tyto úkoly:

a) *„Aby byl pověřenec pro ochranu osobních údajů vyzván k pravidelné účasti na schůzkách vedoucích pracovníků a středního managementu.*
b) *Aby byla přítomnost doporučena při přijímání rozhodnutí, která mají důsledky pro ochranu osobních údajů. Veškeré příslušné informace musí být pověřenci pro ochranu osobních údajů předány dostatečně včas na to, aby mohl poskytovat odpovídající posudky.*
c) *Aby byl stanovisku pověřence pro ochranu osobních údajů vždy přikládán náležitý význam. V případě neshody pracovní skupina WP29 jako osvědčený postup doporučuje doložit důvody, proč nebyl posudek pověřence pro ochranu osobních údajů dodržen.*
d) *Aby byl pověřenec pro ochranu osobních údajů konzultován, jakmile by došlo k porušení ochrany údajů nebo jinému incidentu“* [85]

V zásadě se dá shrnout, že hlavní důvod pro zavedení pověřence pro ochranu osobních údajů je, aby fungoval jako zprostředkovatel mezi dozorovým úřadem, správcem a subjekty údajů, tedy jak už jsem výše naznačil, je to „ombudsman“ osobních údajů.

4.2 Potřebnost institutu u orgánů veřejné moci

V první fázi si musíme uvést, že povinnost jmenovat pověřence pro ochranu osobních údajů se nevztahuje na všechny správce osobních údajů, jsou to zejména správci, kteří jsou uvedeni v článku 37. Důvody pro zavedení institutu pověřence pro ochranu osobních údajů je více.

a) *„Orgán veřejné moci s výjimkou soudů či veřejný subjekt, s výjimkou soudů, které operují v rámci svých soudních pravomocí.*
b) *Hlavní činností správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů.*
c) *Hlavní činností správce nebo zpracovatel spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 GDPR a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů v článku 10 GDPR.*“[86]

V této kapitole se zaměříme zejm. na bod a), je třeba si vůbec vymezit, co to je orgán veřejné moci. Smlouva o fungování EU žádný takový pojem nedefinuje, pouze operuje

[85] Pokyny Pracovní skupiny 29 týkající se pověřenců pro ochranu osobních údajů ze dne 13. prosince 2016, s. 16.

[86] Čl. 37 odst. 1 písm. a) – c).

s pojmem veřejná moc, nezakládá však definici, kdo a jaký subjekt působí jako orgán veřejné moci. Nezbyde nám nic jiného než vyjít z národní úpravy, to znamená, že veřejná moc je taková moc, která autoritativně rozhoduje o právech a povinnostech[87], a to přímo, nebo zprostředkovaně. Dalším kritériem je také, že subjekt, který rozhoduje, není v rovnoprávném postavení, jako subjekt o kterém je rozhodováno.[88] Zároveň veřejnou moc lze členit na státní moc a ostatní veřejnou moc, ostatní veřejná moc je odlišná tím, že nositelé jsou osoby odlišné od státu, tedy další osoby veřejného i soukromého práva.[89] Definice je dle mého názoru široká a je dost možné, že pro účely acquis communautaire bude zúžena.

Dle současného výkladu potřebují pověřence všechny mateřské školky, základní školy, obce a kraje, zároveň i profesní komory jako je advokátní komora. Já ale tvrdím, že takový výklad není úplně správný a pokulhává v oblasti školství. Pověřence pro ochranu osobních údajů nemusí mít všechny školy. Metodika MŠMT stanoví přesně opak, že všechny školy a školská zařízení musejí mít pověřence pro ochranu osobních údajů – „*Čl. 37 odst. 1 písm. a) nařízení stanovuje, že správce a zpracovatel jmenují pověřence v každém případě, kdy zpracování provádí orgán veřejné moci či veřejný orgán, s výjimkou soudů jednajících v rámci svých soudních pravomocí. Školy a školská zařízení za „orgány veřejné moci" ve smyslu nařízení označit lze, neboť v jistých situacích mají pravomoc rozhodovat o právech a povinnostech fyzických osob. Z tohoto důvodu všechny školy a školská zařízení mají povinnost jmenovat pověřence pro ochranu osobních údajů*" [90]. Tedy v této výkladové praxi orgány veřejné moci vymezujeme tak, že jde o vykonavatele veřejné správy, kteří rozhodují o právech a povinnostech zejména ve správním řízení – autoritativně rozhodují o právech a povinnostech, jak bylo popsáno výše.

S metodikou ale nelze souhlasit, jako dobrý příklad můžou sloužit např. základní umělecké školy, které jsou správci osobních údajů a GDPR jako takové se na ně vztahuje. Nicméně povinnost mít pověřence na ně dle mého názoru nedopadá a MŠMT se mýlí. Ve školské praxi byla totiž otázka aplikace správního řádu vždy poněkud zrádná, nad povinnosti, co stanoví školský zákon, judikatura správních soudů roztáhla užití správního řízení na pestrou směsici úkonů škol a školských zařízení (včetně odepření veganské stravy ve školní jídelně)[91]. Pro účely určení existence povinnosti mít pověřence však nelze vycházet z dojmů nastolených judikaturou, ale musíme se opřít o pokud možno objektivní hlediska, naplňující

[87] Usnesení Ústavního soudu ze dne 25. 11. 1993 sp. zn. II. ÚS 75/93.

[88] Tamtéž.

[89] SLÁDEČEK, V. *Obecné správní právo. 3. aktualizované a upravené vydání*. Praha: Wolters Kluwer ČR, 2013, s. 27.

[90] Ministerstvo školství, mládeže a tělovýchovy. *Metodická pomůcka k aplikaci GDPR,* s. 74.

[91] Rozsudek Nejvyššího správního soudu ze dne 5. května 2011 sp. zn. 2 Aps 3/2010, s. 9

požadavky na právní jistotu a odpovídající povaze a účelu institutu pověřence. V tomto případě směřuji k výkladu, že pověřence musejí mít ty školy, které rozhodují ve věcech uvedených v § 165 odst. 2 školského zákona.

Na ZUŠ toto ustanovení nedopadá, pouze s výjimkou zamítnutí žádosti individuálního vzdělávacího plánu, vyloučení nebo podmínečného vyloučení ze vzdělání. Toto ustanovení nelze brát izolovaně a je třeba brát vždy v kontextu dalších předpisů[92]. Tedy rozhodování ZUŠ dle § 165 odst. 2 školského zákona lze považovat za tak nahodilou a okrajovou záležitost, že by bylo nepřiměřené formalisticky z nich dovozovat povinnost mít pověřence. To samé platí i v případě Dětských domovů mládeže či klasických dětských domovů. Zde zdůrazňuji, že v českém prostředí se kvůli rozsáhlosti aplikace správního řádu formálně vzato dostává do zóny s povinností mít pověřence nedůvodně mnoho malých správců osobních údajů.

Dovolím si tvrdit, že z věcného hlediska je na pováženou i to, že pověřence musejí mít malé obce (cca do 300 obyvatel) nebo malé mateřské školy (zde dle mého právního názoru ale nelze najít jiný způsob, jak těmto správcům od této povinnosti ulevit), proto si myslím, že je důvodné být ve výkladu umírněný a nevykládat toto ustanovení extenzivně, ale naopak, postupovat restriktivním a umírněným výkladem a ulevit tím některým druhům škol a školských zařízení.

4.3 Zhodnocení efektivity činnosti pověřence při aplikaci institutu na obce

4.3.1 Úkoly pověřence

V rámci efektivního zakotvení institutu pověřence ve veřejné správě jsou důležité úkoly, které pověřenci z nařízení vyplývají, těmi nedůležitějšími jsou:

a) Poskytování informací a poradenství správcům (zpracovatelům) o jejich povinnostech podle GDPR a dalších předpisů Unie nebo členských států v oblasti ochrany osobních údajů.
b) Monitorování souladu s obecným nařízením.
c) Poskytování poradenství na požádání.
d) Spolupráce s dozorovým úřadem a působení jako kontaktní místo pro dozorový úřad.[93]

[92] MORAVEC, Josef. In RIGEL, Filip, BAHÝĽOVÁ, Lenka, KUDROVÁ, Veronika. *Školský zákon: komentář*. Praha: C.H. Beck, 2014. s. 730.

[93] MATOUŠOVÁ, Miroslava. *Pověřenec pro ochranu osobních údajů.* Presentation presented at [Konzultace pro pověřence pro ochranu osobních údajů jmenovaných dle čl. 37 odst. 1. písm. a]. Úřad pro ochranu osobních údajů, 9. října 2018.

Tyto čtyři povinnosti by měl pověřenec vykonávat na základě svých odborných kvalit a nezávislým způsobem. Definice odborné nebo profesní kvality pro výkon funkce pověřence není nikde taxativně určen, hlavní faktor má být, že pověřenec má mít znalosti v oblasti vnitrostátní a evropské legislativy a zároveň musí mít důkladnou znalost nařízení. Důležité je, aby pověřenec měl takové znalosti, aby řádně rozuměl operacím zpracování, které provádí správce (nejen v právním slova smyslu, ale aby alespoň částečně rozuměl informačním systémům a potřebám správce).[94] V praktickém slova smyslu to znamená, že pověřenec pro nemocnici bude muset mít zásadně vyšší kvalifikaci než pověřenec pro malou obec. Zároveň k tomu dodávám, pokud jde o orgán veřejné moci, je vhodné, aby pověřenec měl elementární znalost postupů v dané instituci. Tedy pokud půjde o školu, aby měl znalost školského zákona a správního řádu, pokud o obce, je důležité, aby měl znalost zákona o obcích, správního řádu a dalších právních předpisů, které se správce (obce) týkají. Povinnosti, které můžou některým správcům působit potíže, jsou záznamy o činnostech zpracování dle čl. 30. Jde o náhradu povinností § 18 odst. 2, případně § 16 zákona o ochraně osobních údajů[95].

Záznamy o činnostech zpracování mají dvojí funkci, interní a externí, první slouží přímo pro pověřence pro ochranu osobních údajů. Dá se říct, že záznam slouží jako mapa nebo orientační plán, externí funkce pak slouží pro ÚOOU, subjekty údajů v určitých případech apod. Záznamy pověřenci musejí být trvale přístupné, otázkou pak bude případná odpovědnost pověřence pro ochranu osobních údajů. Domnívám se, že pověřenec pro ochranu osobních údajů by měl nést odpovědnost za vedení záznamů přinejmenším implicitně, pověřenec je kontaktním místem pro dozorový úřad, tedy odpovědnost dovozuji dle čl. 30 odst. 4 ve spojení s čl. 39 odst. 1 písm. d) GDPR, které stanoví, že na požádání je třeba poskytnout záznamy dozorovému úřadu[96], tedy on bude vysvětlovat případné nesrovnalosti v záznamech o činnostech, které slouží ke komunikaci se subjekty údajů. GDPR v čl. 15 obecně zakotvuje práva subjektů údajů, kde subjekt údajů má možnost získat informaci od správce, jestli jsou předmětné osobní údaje zpracovávány (včetně přístupu k těmto informacím.)[97] v rámci vyřizování práv subjektů údajů bude docházet ke kolizi s informačním zákonem.

---

[94] Pokyny Pracovní skupiny 29, *týkající se pověřenců pro ochranu osobních údajů ze dne* 13. prosince 2016, s. 13

[95] zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

[96] MATOUŠOVÁ, Miroslava. *Pověřenec pro ochranu osobních údajů.* Presentation presented at [Konzultace pro pověřence pro ochranu osobních údajů jmenovaných dle čl. 37 odst. 1. písm. a]. Úřad pro ochranu osobních údajů, 9. října 2018.

[97] Ministerstvo vnitra. *Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR*. [online]. mvcr.cz, 2017. [cit. 1. prosince 2018]. Dostupné na < https://www.mvcr.cz/gdpr/soubor/stanoviska-ministerstva-vnitra-k-souvislostem-vyrizovani-zadosti-o-pristup-k-osobnim-udajum-podle-cl-15-gdpr.aspx>.

4.3.2 Kolize norem ochrany soukromí, práva na informace a použitelnost správního řádu

Zde bude docházet ke kolizi mezi čl. 15 GDPR a obecnou úpravou informačního zákona. Otázkou vůbec je, zda je možné na žádosti v režimu obecného nařízení použít správní řád. Čl. 15 zakotvuje právo subjektu údajů získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou nějakým způsobem zpracovávány správcem a pokud ano, tak jakým. Adaptační zákon k GDPR v některých případech totiž předpokládá, že v rámci uplatnění některých práv bude třeba použít správní řád (změna zákona o organizaci v rámci sociálního zabezpečení, ale výslovně neupravuje použití správního řádu[98]. Samo MV ČR uvádí, že tato úprava se použije ve vztahu k ochraně proti zpracování osobních údajů, nikoliv k právnímu režimu přístupu k informacím dle čl. 15[99].

Správní řád není použitelný jen ve správním řízení, ale je použitelný rovněž na jiné činnosti veřejné správy (typicky ověřování, vydávání posudků apod.)[100], pořád to tedy ale znamená, že správní řád bude použit na vrchnostenskou veřejnou správu, nikoliv v soukromoprávní rovině. K tomu lze dodat, že zákon o ochraně osobních údajů předpokládal podobné informační právo subjektu údajů a zároveň tento zákon neřešil vztah ke správnímu řádu.[101] Tento problém již byl řešen soudní judikaturou a šlo o poskytnutí informací o všech osobních údajích vůči finančnímu úřadu, soud se vůbec nezabýval otázkou, jestli jde o soukromoprávní vztah, či jde o vztah s výkonem vrchnostenské veřejné správy, jelikož jde automaticky o soukromoprávní věc[102].

Tato judikatura je použitelná a v rámci právního režimu obecného nařízení lze vztáhnout i na výkon práv dle čl. 15. Ustanovení totiž nejsou výkonem veřejné moci, případně nějaké vrchnostenské správy, ale soukromoprávní záležitostí, tedy se správní řád nepoužije. Samozřejmě je třeba odlišovat výkon Úřadu pro ochranu osobních údajů, který může projednat stížnosti/přestupky, na toto jednání jednoznačně správní řád dopadá (včetně

---

[98] *Důvodová zpráva k návrhu zákona o zpracování osobních údajů* [online]. Úřad vlády České republiky, 2018 [cit. 1. prosince 2018]. Dostupné na <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

[99] Ministerstvo vnitra. *Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR*. [online]. mvcr.cz, 2017. [cit. 1 prosince 2018]. Dostupné na < https://www.mvcr.cz/gdpr/soubor/stanoviska-ministerstva-vnitra-k-souvislostem-vyrizovani-zadosti-o-pristup-k-osobnim-udajum-podle-cl-15-gdpr.aspx>.

[100] JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád: komentář*. 5. vydání. V Praze: C.H.Beck, 2016, s. 17.

[101] Ministerstvo vnitra. *Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR*. [online]. mvcr.cz, 2017. [cit. 2. prosince 2018]. Dostupné na < https://www.mvcr.cz/gdpr/soubor/stanoviska-ministerstva-vnitra-k-souvislostem-vyrizovani-zadosti-o-pristup-k-osobnim-udajum-podle-cl-15-gdpr.aspx>.

[102] Rozsudek Nejvyššího správního soudu ze dne 6. listopadu 2014, č. Konf 19/2014-7.

zanedbání plnění informační povinnosti dle čl. 13, 15 obecného nařízení.[103] Druhým praktickým bodem, který může bránit efektivnímu výkonu veřejné správy je střet GDPR a informačního zákona. K tomuto bodu nám pomůže negativní vymezení v § 2 odst. 3 informačního zákona, které stanoví, kdy se informační zákon nevztahuje na určitý okruh subjektů. Dva jsou vymezeny výslovně, těmi jsou údaje v centrální evidenci účtů a navazujících evidencí a poskytování informací, které jsou předmětem průmyslového vlastnictví.[104]

Obecněji je již napsáno, že věcná působnost informačního zákona se nebude vztahovat na poskytování informací, pokud zvláštní výkon upraví jejich poskytování., tzn., že „*zvláštní zákony vylučují působnost zákona o svobodném přístupu k informacím upravovat poskytování informací komplexně, včetně procesní stránky a záruky právní ochrany žadatele o informace*“[105] Tedy čl. 15 ve spojení s čl. 12 GDPR naplňuje definiční znaky a možnost aplikace § 2 odst. 3 informačního zákona, jelikož obecné nařízení o ochraně osobních údajů fyzických osob je komplexním právním předpisem. Pokud by subjekt údajů žádal o informace dle čl. 15 GDPR, ale v režimu zákona o svobodném přístupu k informacím, povinný subjekt bude povinen žádost odmítnout dle § 15 odst. 1. Odmítnutí žádosti vychází z judikatury[106]. To však neznamená, že odmítnutou žádost povinný subjekt nemusí vyřizovat, bude ji povinen vyřídit, ale v režimu obecného nařízení.

[103] Ministerstvo vnitra. *Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR*. [online]. mvcr.cz, 2017. [cit. 2. prosince 2018]. Dostupné na <https://www.mvcr.cz/gdpr/soubor/stanoviska-ministerstva-vnitra-k-souvislostem-vyrizovani-zadosti-o-pristup-k-osobnim-udajum-podle-cl-15-gdpr.aspx>.

[104] JELÍNKOVÁ, Jitka. *Zákon o svobodném přístupu k informacím*. Praha: Wolters Kluwer, 2017, s. 21–22.

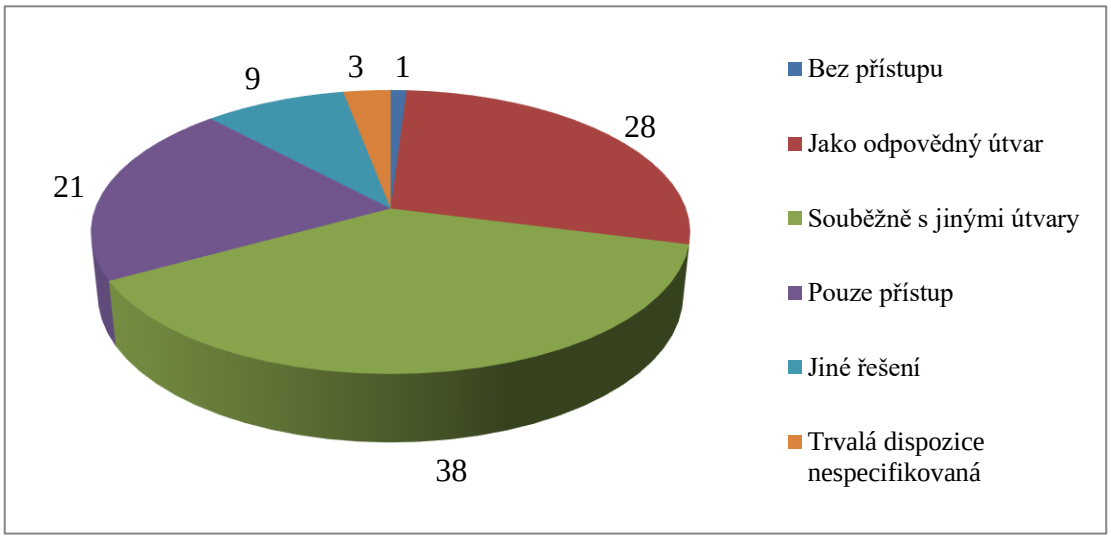
[105] Tamtéž, s. 21.

[106] Rozsudek Nejvyššího správního soudu ze dne č. 9 Ans 7/2012 – 56 ze dne 27. 6. 2012.

4.3.3 Pověřenec a kontakt se správcem a subjekty údajů

Kvalitní a obsahově podrobnou analýzu provedl Úřad pro ochranu osobních údajů, který sesbíral data od jednotlivých pověřenců (jmenovaných dle čl. 37. odst. 1 písm. a) na vzorku 600 správců, pouze v malém procentu konstatoval závažné porušení, zejm., v případech, kdy pověřenec nemá přístup k záznamům o činnostech zpracování. Viz následující graf.

Graf 2: Přístup k záznamům o činnostech podle čl. 30 (%)



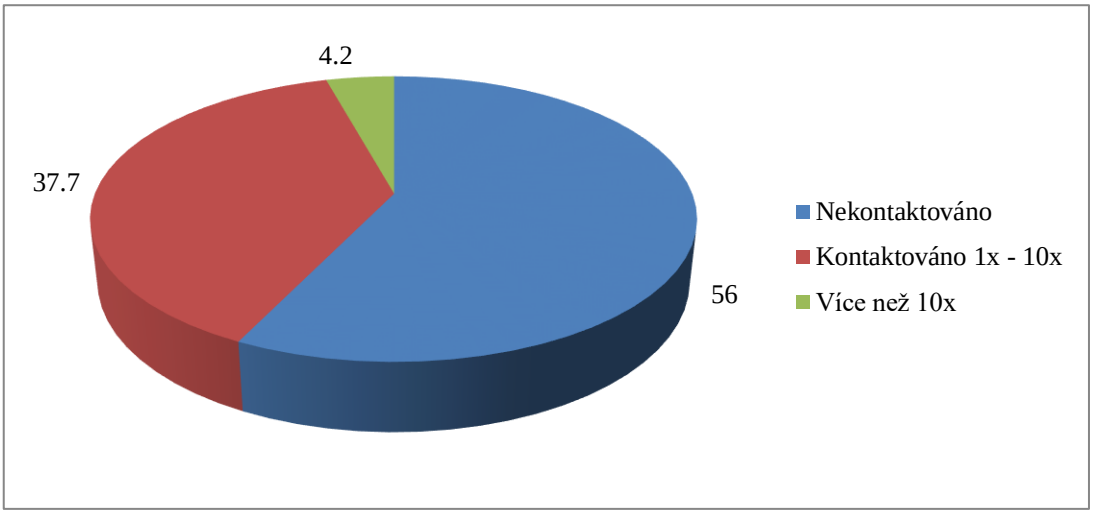
Zdroj:[107]

Zároveň pro efektivní naplnění souladu s GDPR je důležitý kontakt pověřence s vedením správce osobních údajů, tzn., že je vhodné, aby se pravidelně setkával s vedením. Kontakt s vedením pravidelně naplňuje 79 % správců osobních údajů, 2, 6 % je stanoveno takové setkávání jako budoucí a setkávání pouze na základě rozhodné události je u 14 % správců. Zajímavé na tomto průzkumu je, že 9 % uvedlo, že se setkává jiným způsobem.[108] Zároveň dosud nebyla většina správců kontaktována subjekty údajů, což mě i přes mediální kampaň upřímně překvapuje. Viz přiložený graf.

[107] MATOUŠOVÁ, Miroslava. *Pověřenec pro ochranu osobních údajů.* Presentation presented at [Konzultace pro pověřence pro ochranu osobních údajů jmenovaných dle čl. 37 odst. 1. písm. a]. Úřad pro ochranu osobních údajů, 9. října 2018.

[108] Tamtéž.

Graf 3: Kontakt se subjekty údajů (%)



Zdroj:[109]

Dovolím si tvrdit na základě předložených dat, že implementace GDPR ve všech veřejných subjektech implementace GDPR činila určité obtíže. Už jen to, že 21 % správců má pouze přístup k záznamům o činnostech lze považovat za alarmující.

[109] MATOUŠOVÁ, Miroslava. *Pověřenec pro ochranu osobních údajů.* Presentation presented at [Konzultace pro pověřence pro ochranu osobních údajů jmenovaných dle čl. 37 odst. 1. písm. a]. Úřad pro ochranu osobních údajů, 9. října 2018.

5 Předávání osobních údajů

5.1 Režim předávání osobních údajů mimo EU

Předávání osobních do zahraničí je určitě fakt, který zaslouží vyšší míru pozornosti. Předávání v rámci EU je vyřešeno samostatně tím, že obecné nařízení o ochraně osobních údajů je právní předpis s přímým účinkem, tedy je přímo použitelné v členských zemích. Zároveň je třeba mít na paměti, že volný pohyb osobních údajů z důvodu ochrany fyzických osob v souvislosti se zpracováním osobních údajů není omezen, ani zakázán. Správce však vždy musí mít na paměti, že předávání osobních údajů musí být vždy založené na nějakém právním důvodu.[110] Zároveň si také musíme definovat pojem předávání do zahraničí, „*předáváním osobních údajů do zahraničí se rozumí obecně jakékoliv sdělení, zpřístupnění nebo jiné poskytnutí osobních údajů správci nebo zpracovateli ve třetí zemi mimo EU*“.[111]

Problematickým ale může být zveřejnění osobních údajů na internetu, dnešní doba informačních technologií poskytuje každému možnost nahlédnout na osobní údaj, pokud je publikován veřejně na internetu, bez skutečnosti, zda je fyzická osoba na druhém konci světa, či pár kilometrů od zařízení, přes které data dotyčný nahrál. Takovou skutečnost řešil SDEU, který v rozsudku konstatoval, že právě pokud jsou osobní údaje zveřejněny dálkovým přístupem a má k nim přístup v podstatě kdokoliv, nejde o režim předávání osobních údajů do zahraničí[112]. Na světě existují státy s různou mírou ochrany osobních údajů, tomu pak odpovídají jednotlivé způsoby, jak zajistit předání osobních údajů[113].

Obecně princip předávání osobních údajů ale zůstává nezměněný od předchozí právní úpravy,[114] Pokud jde o případy, kdy dochází k přenosu dat mimo území EU, nelze počítat Evropský hospodářský prostor (pro tyto země se bude používat obdobný režim předávání osobních údajů, země budou mít zároveň stejnou úroveň ochrany osobních údajů, jako stanovuje GDPR)[115]. Můžou nastat určité jiné problémy. GDPR obecně dělí země na „bezpečné“, ty stanovuje tzv. seznam, který se nazývá white list - ten aktuálně zahrnuje 12

[110] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 152.

[111] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 373.

[112] Rozsudek SDEU ze dne 6. listopadu 2003 ve věci C-101/01 Bodil Lindquist, bod 26

[113] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 151.

[114] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 374.

[115] VOIGT, Paul, VON DEM BUSSCHE, Paul. *The EU General data protection regulation (GDPR) – A practical guide.* Springer: 2017, s. 116.

zemí (případně jejich části – např. Ostrov Jersey[116]), tyto země se považují za bezpečné a lze osobní údaje do takové země předávat.[117] Evropská komise měla údajně vydat seznam, který by byl opakem white list, ale dosud nebyl zveřejněn na internetových stránkách komise. Pouze je zde draft návrhu komise, který by považoval Japonsko za zemi, která má garantovanou bezpečnost osobních údajů a zároveň probíhají jednání s Jižní Koreou[118].

5.2 Právní důvody ochrany a proces k zajištění předání mimo země EU

V GDPR obecně platí jedno pravidlo pro předávání osobních údajů mimo země EU (případně Evropského hospodářského prostoru), které bylo popsáno výše, pokud dojdeme k jeho aplikaci, lze předávat osobní údaje do třetích zemí mimo EU nebo mezinárodním organizacím pouze pokud daný správce splní podmínky dle čl. 44 a následujících GDPR, jinými slovy, lze předat osobní údaje. Pokud existuje alespoň jeden právní důvod, tyto právní důvody lze dělit:

a) Rozhodnutí o odpovídající ochraně vydané Evropskou komisí.
b) Vhodné záruky, pokud se jedná o předávání do země nebo mezinárodní organizace, ve které jsou k dispozici vymahatelná práva subjektů údajů a účinná právní ochrana subjektů.
c) Výjimky pro specifické situace dle čl. 49.[119]

Nařízení správci ale neumožňuje volný výběr z těchto důvodů: první musí zjišťovat, zda existuje rozhodnutí Evropské komise. Pokud není, může využít nějakého ze způsobu vhodných záruk, pokud správce dojde k výkladu, že nelze použít jednu z vhodných záruk, lze použít výjimku dle čl. 49, pokud ani to ne, předání není možné.[120] K první možnosti předání jde o výlučnou pravomoc komise, která může rozhodnout a stanovit, že konkrétní stát, mezinárodní organizace, nebo určitý sektor má adekvátní míru ochrany osobních údajů. Současný seznam zemí, kterým komise dala stanovisko „bezpečné země“ zůstává v účinnosti[121]. Před účinností to byly země: Andora, Argentina, Kanada (za předpokladu

[116] EUROPEAN COMISSION, *Draft adequacy decision.* [online]. ec.europa.eu, 2017. [cit. 2. prosince 2018]. Dostupné na: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>.

[117] Ministerstvo průmyslu a obchodu. *Příručka pro přípravu malých a středních firem na GDPR*, s. 20.

[118] EUROPEAN COMISSION, *Draft adequacy decision.* [online]. ec.europa.eu, 2017. [cit. 2. prosince 2018]. Dostupné na: <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>.

[119] ČL. 44 a násl. GDPR.

[120] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 374.

[121] MOLE Ariane, MULLOCK, James, BOARDMAN, Ruth. *Guide to the General Data Protection Regulation* [online]. Twobirds.com, 2017 [cit. 5. prosince 2018]. Dostupné na

účasti v PIPEDA)[122], Švýcarsko, Faerské ostrovy, Guernsey, Izrael, Ostrov Mann, Jersey, Východní republika Uruquay a Nový Zéland. Předpoklady k tomu, aby bylo vydáno kladné stanovisko, lze najít v recitálu obecného nařízení. K čemu by komise měla přihlížet je pro předávání velice zásadní, v recitálu je stanoveno, že EK se musí řídit se základními hodnotami, na kterých je EU založena s velkým ohledem na lidská práva. V případě úvahy o vydání takového rozhodnutí by EK měla vzít v potaz, jak třetí země dodržuje zásady právního státu, veřejné bezpečnosti. Třetí země by také sama měla nabídnout odpovídající úroveň ochrany osobních údajů, tedy stejnou ochranu jako má EU. Země by také měla být nezávislý dozor, který kontroluje soulad s osobními údaji, nejlépe ve formě dozorového úřadu[123].

Některá ustanovení tohoto recitálu vidím jako problematická, zvlášť z politických důvodů (velice těžko takový status získá země jako Ukrajina, kde probíhá válečný konflikt). Rozhodnutí Komise má určité náležitosti, které musí obsahovat, je to zejm. územní rozsah, také se rozhodnutí může vztahovat jen na určitou část území některého státu. Dále by v obsahu rozhodnutí mělo být, jaký orgán bude poskytovat potřebnou součinnost subjektům údajům a zároveň by mělo být stanoveno, jaký orgán může být kontaktním místem pro dozorové úřady jednotlivých států. Komise má zároveň i povinnost monitorovat průběžně vývoj v třetích zemích a mezinárodních organizacích za účelem posouzení do jaké míry může být ovlivněna úroveň ochrany osobních údajů. Případná změna nemá zpětné účinky[124].

Rozhodnutí EK podléhá Nařízení EU a Evropského parlamentu č. 182/2011 – dle čl. 5, případně dle čl. 8, tzn., že pokud hrozí nebezpečí z prodlení, Evropská komise může vydat rozhodnutí bez předchozího projednání ve výboru.[125] V případě zrušení nebo změny rozhodnutí Komise sama Komise zahájí diskuzi, která povede k nápravě okolností. Pokud správce zjistí, že neexistuje rozhodnutí Evropské Komise, jak již bylo zmíněno, další možností, je předat osobních údaje tzv. na vhodných zárukách. Čl. 46 dělí vhodné záruky na dvě kategorie. Prvními lze předávat osobní údaje bez dalšího, těmi jsou:

a) Právně závazné a vymahatelné nástroje mezi orgány veřejné moci nebo veřejnými subjekty.

<https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>

[122] Program k předávání osobních údajů.

[123] Bod 104 Recitálu GDPR

[124] ČERNÝ, Jiří. In PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018, s. 329.

[125] NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí. L 55/13.

Tento institut se primárně použije v rámci bilaterálních vztahů mezi EU a třetími státy, typickým příkladem může být „Passenger Name Record – PNR“, dohoda mezi EU a USA o předávání jmenných seznamů cestujících. Dnes již PNR má formu směrnice, která byla schválená 21. dubna 2016[126], členské státy měly dva roky na implementaci této směrnice. Dohody vznikají zejm. k odhalování nezákonných finančních transakcí a pro účely programu sledování terorismu.[127]

b) Závazná podniková pravidla (BCR).[128]

   Závazná podniková pravidla mají dva druhy. Závazná podniková pravidla pro správce (BCR – P) a pro zpracovatele (BCR – P)[129], záleží tedy, v jakém postavení je jednotlivá organizace, která musí BCR aplikovat.[130] Toto použití bude zejména v nadnárodních korporacích. Vodítka skupiny WP29 vyloženě operují s dvěma pojmy, které se týkají těchto podnikatelských aktivit - „Group of undertakings“ a „group of enterprises engaged in a joint economic activity“, ve volném překladu skupina podnikatelů a skupina vykonávající podobnou ekonomickou činnost.[131]

c) Standardní smluvní doložky.

   Smluvní doložka nemusí být uzavřena jako jednotlivá smlouva, většinou se uzavírají smlouvy, které mají hospodářský charakter (souvisí s hospodářským důvodem závazku). Nejlepším řešením je smluvní klauzule přímo ustanovit v textu smlouvy, které definuje zpracování osobních údajů. [132]

d) Schválený kodex chování.

   Je jednou z vhodných záruk. Problematické, ale může být, že i u těchto záruk je třeba zajistit závazné a vymahatelné závazky správce/zpracovatele, tedy použití tohoto institutu nemusí být vždy výhodné.

e) Schválený mechanismus pro vydání osvědčení podle článku 42 spolu se závaznými a vymahatelnými závazky správce nebo zpracovatele ve třetí zemi uplatňovat vhodné záruky, a to ohledně práv subjektu údajů.

---

[126] Lze konstatovat, že v dubnu 2016 Parlament EU a Rada EU schválila „balíček“ předpisů o ochraně osobních údajů.

[127] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 384.

[128] Binding corporate rules.

[129] Controller je anglický ekvivalent pro správce, proto zkratka C, processor je anglický ekvivalent pro zpracovatele, proto zkratka P.

[130] SUCHÁNKOVÁ, Lenka. In PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018, s. 338–340.

[131] Vodítka Pracovní skupiny 29 č. WP257, *Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules,* s. 1–3.

[132] ČERNÝ, Jiří. In PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018, s. 334.

Další kategorií jsou záruky, které musí schválit dozorový úřad, musí postupovat dle mechanismu čl. 63 a násl. GDPR.

a) Vlastní smluvní doložky mezi správcem nebo zpracovatelem v EU a správcem, zpracovatelem nebo příjemcem ve třetí zemi nebo v mezinárodní organizaci.
b) Ustanovení určená k vložení do správních ujednání mezi orgány veřejné moci nebo veřejnými subjekty, která zahrnují vymahatelná a účinná práva subjektů údajů.

Takový složitý proces může v rámci některých osobních údajů vypadat jako zbytečný, ale tato rozhodnutí jsou pro Evropskou unii důležitá i z politického a bezpečnostního hlediska. EU jako politická a ekonomická unie je v dnešním digitálním světě vystavována poměrně velkým hrozbám, které se týkají informací a práce s nimi. Potencionální hrozby budou rozebrány v předposlední podkapitole.

5.3 Programy Evropské komise k zajištění rychlejšího předávání mimo země EU

Programy Evropské komise, které budou v této práci zmíněny, se týkají zejm. obchodu EU a USA. První program, který byl účinný, byl tzv. Safe Harbour. Safe Harbour byl přijat dne 26. července 2000 rozhodnutím EK č. 2000/520/ES. Původním rozhodnutím se měla zlepšit ochrana osobních údajů mezi EU a USA. USA v této době obecně měly nižší míru ochrany osobních údajů než EU[133] a uplatňovaly i trochu jiný systém, tzv. odvětvový přístup – ten byl založen na kombinaci různých principů (právní předpisy, samoregulace atd).[134] K předání osobních údajů, které byly na seznamu Safe Harbour, se nevyžadovalo povolení dozorového úřadu, což byla značná výhoda.[135] Tento program byl účinný do roku 2013, zrušen byl na základě žaloby M. Schremse, rakouský občan M. Schrems, v té době ještě student, podal stížnost ke společnosti Facebook Ireland. Důvodem pro podání žaloby byla kauza PRISM, kdy Americká NSA měla velký přístup k datům napříč Evropou. M. Schrems zdůvodnil, že takové předávání nemá opodstatněný právní základ, tedy stížnost byla podána přímo k irskému komisaři pro ochranu osobních údajů. Tato stížnost byla zamítnuta, ale v důsledku další žaloby M. Schremse směřovala k Vrchnímu soudu v Irsku.[136] Ten řízení

[133] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 326.

[134] Tamtéž

[135] ÚOOU. *Stanovisko 2/2010 Předání osobních údajů do jiných států*. [online]. uoou.cz listopad 2010. [cit. 5. prosince 2018]. Dostupné na <https://www.uoou.cz/files/stanovisko_2010_2.pdf>.

[136] DONÁT, Josef. *Rozhodnutí SDEU ve věci Schrems: zneplatnění systému Safe Harbour a jeho důsledky pro předávání dat do USA.* [online]. tablet.epravo.cz, říjen 2015. [cit. 5. prosince 2018]. Dostupné na: <https://tablet.epravo.cz/10-2015/komentare-rozhodnuti-sdeu-ve-veci-schrems-zneplatneni-systemu-safe-harbor-a-jeho-dusledky-pro-predavani-dat-do-usa/>.

pozastavil a podal předběžnou otázku k SDEU, kde se tázal, zda irský komisař je vůbec oprávněn přezkoumávat podmínky ochrany osobních údajů.

Ve svém řízení SDEU zejména podoktl princip, který opakuje ve své judikatuře, že aby došlo k důslednému naplňování práva na respektování soukromého života, je možné využít výjimky, které jsou jen naprosto nezbytné k naplnění takového cíle.[137] SDEU sám ještě v řízení o předběžné otázce zkritizoval, že rozhodnutí Safe Harbour reálně nezajišťuje ochranu osobním údajům v rámci svých vnitrostátních/mezinárodních závazcích. Program také dával přednost veřejnému zájmu a zájmu jednotlivých států před ochranou předávání osobních údajů, tím byl orgánům USA poskytnut přístup v rámci e-komunikace.[138] Program Safe Harbour byl na základě těchto zrušen.[139] Po zrušení tohoto rozhodnutí došlo k diskuzi, jakým stylem předávat dál osobní údaje do USA. Evropská unie a Spojené státy americké mají velmi úzké obchodní styky, tedy je nutné zajistit přechod osobních údajů mezi EU a USA, tím se vytvořila myšlenka dalšího programu EK. Spojené státy americké mají trochu odlišné postavení, jsou totiž na seznamu EK, ale nikoliv jako stát jako celek, ale pouze vůči jednotlivým příjemcům osobních údajů, kteří se účastní programu Privacy Shield.

Po zrušení Bezpečného přístavu proběhla velké debata mezi oběma celky (EU a USA), jakým způsobem nastavit nová pravidla. Legislativní jednání proběhla na úrovni i skupiny WP29 a evropského komisaře pro ochranu osobních údajů.[140] Nakonec byl přijat program Privacy shield, který funguje na principu volného přihlášení[141], zároveň seznam amerických společností, které se do programu zapojily, lze dohledat volně na internetu.[142] Tyto společnosti, které se přihlásily do programu Privacy shield, se zavázaly dodržovat i zásady tohoto programu, v zásadě je ale na konkrétních podnicích, aby takovou praxi zavedly.

---

[137] ROZSUDEK SOUDNÍHO DVORA (velkého senátu): „Elektronické komunikace – Směrnice 2006/24/ES – Veřejně dostupné služby elektronických komunikací nebo veřejných komunikačních sítí – Uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním takových služeb – Platnost – Články 7, 8 a 11 Listiny základních práv Evropské unie“ [online]. Curia.europa.eu, 8. dubna 2014 [cit. 5. prosince 2018]. Dostupné na <http://curia.europa.eu/juris/document/document.jsf;jsessionid=B5808551F12A512B3680255D8D72CCB3?text=&docid=150642&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=2705095>

[138] DONÁT, Josef. *Rozhodnutí SDEU ve věci Schrems: zneplatnění systému Safe Harbour a jeho důsledky pro předávání dat do USA.* [online]. tablet.epravo.cz, říjen 2015. [cit. 5. prosince 2018]. Dostupné na: <https://tablet.epravo.cz/10-2015/komentare-rozhodnuti-sdeu-ve-veci-schrems-zneplatneni-systemu-safe-harbor-a-jeho-dusledky-pro-predavani-dat-do-usa/>.

[139] Soudní dvůr: Rozsudek ze dne 6. října 2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14, bod 104.

[140] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 378.

[141] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018, s. 154.

[142] Lze dohledat aktivní i neaktivní společnosti na odkazu: https://www.privacyshield.gov/list.

V případě nedodržení je možné udělit sankci od Federální obchodní komise USA[143], tedy od jiného orgánu než evropského. To z podstaty vidím jako problematické zejm., v nemožnosti řádné kontroly evropských orgánů. Privacy shield byl také v řízení před soudem. Během přijímání nového programu zaznívaly názory, že by mělo dojít k jeho zpřísnění, a to ze stejného důvodu jako v programu Safe Harbour, z přístupu veřejných orgánů USA. Velká část programu a jeho záruky byly poskytnuty ještě za administrativy Barracka Obamy. Tedy i po nástupu Donalda Trumpa k moci panovaly určité obavy, že tento program může být stažen[144], což se nakonec nestalo. Už v době přijímání skupina WP29 uplatňovala připomínky k programu Privacy shield, zejm. rozhodnutí o odpovídající ochraně, skupina WP 29 kritizuje hlavně, že stěžejní klíčové zásady nejsou právě v rozhodnutí o odpovídající ochraně osobních údajů, případně nebyly dostatečně nahrazeny. V zásadě skupina WP29 kritizuje tyto body:

a) Nejsou jasně uvedeny zásady uchovávání osobních údajů.
b) Neexistuje žádný předpis, který by výslovně chránil automatizované zpracování osobních údajů.
c) Nejasné vymezení zásady účelového omezení.[145]

[143] NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017, s. 379.

[144] Tamtéž.

[145] Stanovisko Pracovní skupiny č. 17/EN/WP255, *EU – U.S. Privacy Shield – First annual Joint Review,* s. 10–15.

6 Závěr

GDPR pro představitele malých obcí a správců znamenalo de facto revizi/audit v dokumentech, které obsahují osobní údaje. Dle popsaných povinností v kapitole tři, včetně informací od správců osobních údajů, které jsem oslovil dle informačního zákona lze konstatovat, že GDPR lehce zatížilo orgány veřejné moci ve smyslu finančním a administrativním, museli totiž přijmout některá bezpečnostní opatření, vynaložit část svých finančních prostředků na revizi dokumentů a věnovat svůj čas této problematice. Já osobně vidím povinnosti, které GDPR ukládá jako odpovídající dnešnímu digitálnímu světu.

Dovolím si konstatovat, že u většiny správců implementace proběhla a své povinnosti vyplývající z nařízení dodrželi nebo se aspoň snaží dodržet. Dle žádostí, které jsem podal podle informačního zákona lze vycítit značnou nechuť subjektů k dalšímu administrativnímu nárůstu, to je problematické, ale u každého předpisu, který stanovuje nové povinnosti.

V rámci zpracovatelských smluv jsem zaznamenal jediný možný problém a to je možné nadbytečné užívání zpracovatelských smluv, ne vždy při uzavírání smlouvy mezi orgánem veřejné moci a některým externím subjektem bude naplněn čl. 28. Často půjde o čl. 29, nikoliv čl. 28 GDPR, tedy externí subjekt nebude mít postavení zpracovatele, ale pouze subjektu, který koná zpracování z pověření správce. To je poměrné zásadní v důsledku povinností, pokud půjde o zpracovatelskou smlouvu, ve velkém procentu případů bude zpracovatel mít povinnost vést záznamy o činnostech, což znamená zvýšenou administrativní zátěž. Orgány veřejné moci by si při každém uzavírání smlouvy měli důsledně zvážit, jestli jde o typ činností a jestli je opravdu nutné postupovat dle čl. 28.

Problematická mohla být kolize hodnot mezi informačním zákonem a GDPR. Tyto předpisy se budou protínat ve velké míře, protože pokud někdo žádá informace o nějaké osobě, bude žádat jeho/její osobní údaje. Pokud by ale žádal o informace v režimu informačního zákona a uplatňoval by v žádosti práva z GDPR, povinný subjekt bude povinen takovou žádost odmítnout a vyřizovat v režimu GDPR, nikoliv v režimu obecného nařízení. To si myslím, že je vhodné, zejména pro pověřence pro ochranu osobních údajů, protože pověřenec jako nezávislý orgán by neměl vyřizovat žádosti dle informačního zákona, tím by mohla být narušena nezávislost pověřence.

U pověřence pro ochranu osobních údajů vidím problematické jmenování pověřence u orgánů veřejné moci. Již jednou jsem zmínil, že se do takové zóny dostává nedůvodně mnoho malých správců osobních údajů. Zákonodárce se již v legislativním procesu měl zamyslet, jestli je vhodné mít takto rozsáhlou definici dle § 37 odst. 1 písm. a). Po účinnosti GDPR již nevidím možnost, která by z této definice odstranila malé orgány veřejné moci, musím ale

konstatovat, že ustanovení čl. 37 odst. 1 písm. a) není vhodné pro země, které mají tak širokou aplikaci správního řádu jako právě Česká republika.

K předávání osobních údajů do zahraničí zásadně nemám výtky mimo to, že rozhodnutí EK je procesně, u některých států tak složité, že nebude v praxi použitelné.

Seznam grafů

Seznam příloh

Seznam použitých zdrojů

1) Knižní publikace

BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 2. vyd. Praha: Linde, 2001.

FIALA, Zdeněk a kol. *Správní právo trestní*. Praha: Leges, 2017.

HENDRYCH, Dušan a kol. *Správní právo. Obecná část.* 4. Vydání, Praha: C. H. Beck, 2001.

JANEČKOVÁ, Eva. *GDPR: praktická příručka implementace*. Praha: Wolters Kluwer, 2018.

KOLMAN, Petr, *Úvahy o veřejném právu*. Praha: Leges, 2014.

SLÁDEČEK, Vladimír, POUPEROVÁ, Olga. *Správní právo: zvláštní část (vybrané kapitoly)*. 2. Vydání. Praha: Leges, 2014.

NEZMAR, Luděk. *GDPR Praktický průvodce implementací.* Praha: Grada Publishing, 2017.

SLÁDEČEK, V. *Obecné správní právo. 3. aktualizované a upravené vydání*. Praha: Wolters Kluwer ČR, 2013.

ŠIŠKOVÁ, Naděžda, STEHLÍK, Václav. *Evropské právo 1 - ústavní základy Evropské unie*. Praha: Linde, 2007.

VOIGT, Paul, VON DEM BUSSCHE, Paul. *The EU General data protection regulation (GDPR) – A practical guide*. Springer: 2017.

TOMÁŠEK, Michal, TÝČ, Vladimír, MALENOVSKÝ, Jiří. *Právo Evropské unie*. 2. aktualizované vydání. Praha: Leges, 2017

ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Olomouc: ANAG, 2018.

2) Internetové zdroje

Adequacy of the protection of personal data in non-EU countries: How the EU determines if a non-EU country has an adequate level of data protection [online]. European Commission [cit. 2. prosince 2018]. Dostupné na <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en>.

Desatero omylů. [online]. uoou.cz, 2017. [cit. 30. listopadu 2018]. Dostupné na <https://www.uoou.cz/desatero-omylu/ds-4818/p1=4818>.

DONÁT, Josef. *Rozhodnutí SDEU ve věci Schrems: zneplatnění systému Safe Harbor a jeho důsledky pro předávání dat do USA* [online]. Epravo.cz, říjen 2015 [cit. 5. prosince 2018]. Dostupné na <https://tablet.epravo.cz/10-2015/komentare-rozhodnuti-sdeu-ve-veci-schrems-zneplatneni-systemu-safe-harbor-a-jeho-dusledky-pro-predavani-dat-do-usa/>.

Důvodová zpráva k návrhu zákona o zpracování osobních údajů [online]. Úřad vlády České republiky, 2018 [cit. 23. listopadu 2018]. Dostupné na <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

FIEGERMAN, Seth. *Google posts its first $100 billion year* [online]. CNN Business,1. února 2018 [cit. 30. listopadu 2018]. Dostupné na <https://money.cnn.com/2018/02/01/technology/google-earnings/index.html>.

HECZKOVÁ, Markéta. *Fakta o obchodě Česka se zahraničím* [online]. statistikaamy.cz, září 2014. [cit. 30. října 2018]. Dostupné na <http://www.statistikaamy.cz/2014/09/fakta-o-obchode-ceska-se-zahranicim/>.

HEJLÍK, Ladislav. *Zpracování osobních údajů v rámci služeb SMS infokanál.* [online]. uoou.cz 13. února 2018. [cit. 30. listopadu 2018]. Dostupné na <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=32116>.

Historie úřadu pro ochranu osobních údajů. [online]. uoou.cz, 2016. [cit. 25. října 2018]. Dostupné na: <https://www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061/p1=1061>.

Jaká je velikost ekonomiky EU? [online]. Europa.eu [cit. 20. listopadu 2018]. Dostupné na <https://europa.eu/european-union/about-eu/figures/economy_cs>.

Kyberbezpečnost – Forbes. Milionové pokuty za únik dat. [online]. kyberbezpecnost.forbes.com, 2017. [cit. 30. října 2018]. Dostupné na: <https://money.cnn.com/2018/02/01/technology/google-earnings/index.html>.

Ministerstvo vnitra. *Stanovisko Ministerstva vnitra k použitelnosti správního řádu v souvislosti s uplatňováním práva subjektu údajů na přístup k osobním údajům podle GDPR.* [online]. mvcr.cz 2017. [cit. 1. prosince 2018]. Dostupné na <

https://www.mvcr.cz/gdpr/soubor/stanoviska-ministerstva-vnitra-k-souvislostem-vyrizovani-zadosti-o-pristup-k-osobnim-udajum-podle-cl-15-gdpr.aspx>.

MOLE Ariane, MULLOCK, James, BOARDMAN, Ruth. *Guide to the General Data Protection Regulation* [online]. Twobirds.com, 2017 [cit. 5. prosince 2018]. Dostupné na <https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en>.

Návrh zákona o zpracování osobních údajů [online]. Aplikace O/dok, 2018[cit. 30. října 2018]. Dostupné na <https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5>.

Nepravdy o wi-fi. [online]. uoou.cz, 2017. [cit. 30. října 2018]. Dostupné na <https://www.uoou.cz/nepravdy-o-wi-fi-v-souvislosti-s-gdpr/d-28774>.

NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 26. října 2018]. Dostupné na: <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.

NEUWIRT, Karel. *Ochrana osobních údajů a vstup do EU.* [online]. uoou.cz, 2003 [cit. 30. října 2018]. Dostupné na: <https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=8087>.

Stanovisko 2/2010 Předání osobních údajů do jiných států. [online]. uoou.cz, listopad 2010. [cit. 5. prosince 2018]. Dostupné na < https://www.uoou.cz/files/stanovisko_2010_2.pdf>.

Stanovisko č. 12/2012 aktualizace říjen 2017 K použití fotografie, obrazového a zvukového záznamu fyzické osoby. [online]. uoou.cz, 20. listopadu 2017. [cit. 26. listopadu 2018]. Dostupné na <https://www.uoou.cz/stanovisko-c-12-2012-k-pouziti-fotografie-obrazoveho-a-zvukoveho-zaznamu-fyzicke-osoby-aktualizace-rijen-2017/d-27693/p1=0>.

ŠKORNIČKOVÁ, Eva. *Správce osobních údajů.* [online]. gdpr.cz, 2018 [cit. 23. listopadu 2018]. Dostupné na: <https://www.gdpr.cz/gdpr/heslo/spravce-osobnich-udaju/>.

Tisková zpráva uoou udělil rekordní pokutu za spam. [online]. uoou.cz, 2017. [cit. 30. listopadu 2018]. Dostupné na: <https://www.uoou.cz/tiskova-zprava-uoou-udelil-rekordni-pokutu-za-nbsp-spam/d-23838/p1=1017>.

Základní příručka k GDPR [online]. uoou.cz, 2018 [cit. 30. října 2018]. Dostupné na

<https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744>.

Zveřejňování osobních údajů studentů [online]. uoou.cz, 18. Dubna 2013 [cit. 25. listopadu 2018]. Dostupné na <https://www.uoou.cz/zverejnovani-osobnich-udaju-studentu/d-1756>.

3) Judikáty

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

Rozsudek SDEU ze dne 19. října 2016, ve věci C-582-14, Patrick Breyer v Bundesrepublik Deutschland

Rozsudek SDEU ze dne 6. listopadu 2003 ve věci C-101/01 Bodil Lindquist

Rozsudek Nejvyššího správního soudu ze dne 6. listopadu 2014, č. Konf 19/2014-7

Rozsudek Nejvyššího správního soudu ze dne č. 9 Ans 7/2012 - 56 ze dne 27. 6. 2012

Rozsudek Evropského soudního dvora ze dne 6. října 1970, *Grad v. Finanzamt Traunstein*, 9/70.

ROZSUDEK SOUDNÍHO DVORA (velkého senátu): „Elektronické komunikace – Směrnice 2006/24/ES – Veřejně dostupné služby elektronických komunikací nebo veřejných komunikačních sítí – Uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním takových služeb – Platnost – Články 7, 8 a 11 Listiny základních práv Evropské unie“ [online]. Curia.europa.eu, 8. dubna 2014 [cit. 5. prosince 2018]. Dostupné na <http://curia.europa.eu/juris/document/document.jsf;jsessionid=B5808551F12A512B3680255D8D72CCB3?text=&docid=150642&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=2705095>.

Rozsudek Nejvyššího správního soudu ze dne 5. května 2011 sp. zn. 2 Aps 3/2010

Soudní dvůr: Rozsudek ze dne 6. října 2015, Maximillian Schrems v. Data Protection Commissioner, C-362/14

4) Právní předpisy a články

Bundesdatenschutzgesetz ze dne 30. června 2017 (BGBI. IS. 2097)

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. Úř. věst. L 119, 4. května 2016

Nařízení Evropského parlamentu a Rady (EU) č 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí

Listina základních práv Evropské unie, 14. 12. 2007, Úřední věstník Evropské unie, C 303/1.

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

zákon č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností

5) Komentáře

HULMÁK, Milan. *Občanský zákoník V: závazkové právo: obecná část (§ 1721-2054):* komentář. Praha: C.H. Beck, 2014.

LAVICKÝ, Petr. *Občanský zákoník: komentář*. Praha: C.H. Beck, 2015.

MELZER, Filip a kol. *Občanský zákoník – velký komentář.* Svazek 1 § 1-117. Praha: Leges, 2013.

PATTYNOVÁ, Jana a kol. *Obecné nařízení o ochraně osobních údajů (GDPR). Data a soukromí v digitálním světě.* Komentář. Praha: Leges, 2018.

RIGEL, Filip, BAHÝĽOVÁ, Lenka, KUDROVÁ, Veronika. *Školský zákon: komentář*. Praha: C.H. Beck, 2014.

JELÍNKOVÁ, Jitka. *Zákon o svobodném přístupu k informacím*. Praha: Wolters Kluwer, 2017.

JEMELKA, Luboš, PONDĚLÍČKOVÁ, Klára, BOHADLO, David. *Správní řád: komentář*. 5. vydání. V Praze: C.H.Beck, 2016.

NULÍČEK, Michal a kol. *Obecné nařízení o ochraně osobních údajů.* Praktický komentář. Praha: Wolters Kluwer, 2017.

6) Stanoviska a zprávy organizací

Stanovisko Working Party 29 č. WP259 k souhlasu dle nařízení 2016/679 ze dne 28. listopadu 2017.

Ministerstvo průmyslu a obchodu. *Příručka pro přípravu malých a středních firem na GDPR*.

Ministerstvo školství, mládeže a tělovýchovy. *Metodická pomůcka k aplikaci GDPR.*

Pokyny Pracovní skupiny 29 „ *pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko*“ pro účely nařízení 2016/679 ze dne 4. Dubna 2017, aktualizované stanovisko 4. října 2017.

Pokyny Pracovní skupiny 29 týkající se pověřenců pro ochranu osobních údajů ze dne 13. Prosince 2016.

Stanovisko Pracovní skupiny WP29– On the principle of accountability – č. 3/2010 ze dne 13. července 2010, s. 4

Vodítka Pracovní skupiny 29 č. WP257, *Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*.

Stanovisko Pracovní skupiny č. 17/EN/WP255, *EU – U.S. Privacy Shield – First annual Joint Review, s. 10–15*

7) Prezentace

MATOUŠOVÁ, Miroslava. *Pověřenec pro ochranu osobních údajů.* Presentation presented at [Konzultace pro pověřence pro ochranu osobních údajů jmenovaných dle čl. 37 odst. 1. písm. a]. Úřad pro ochranu osobních údajů, 9. října 2018.

8) Časopisy

Chládková, Alena. *Osobní údaje v pracovněprávních vztazích.* Práce a mzda, 2018, roč. 66 č. 5, s. 6.

Abstrakt

Práce se zaměřuje na novou právní úpravu ochrany osobních údajů v Evropě. Práce se snaží zanalyzovat důvody zavedení nové právní úpravy a některé nové povinnosti, které zavedlo GDPR. Zaměřuje se na menší správce, hlavně na obce jako orgány veřejné moci.

Diplomová práce také zkoumá uzavírání zpracovatelských smluv mezi správcem a zpracovatelem a jejich aplikační dopady.

Práce zkoumá dopad institutu pověřence pro ochranu osobních údajů a také jestli je potřebné, aby nařízení obsahovalo tak rozsáhlou definici orgánů veřejné moci. Dále se práce zaměřuje na potřebnost institutu pověřence u orgánů veřejné moci a na kontakt pověřence se správci osobních údajů.

V posledním bodě se práce zaměřuje na předávání osobních údajů do zahraničí.

Abstract

Theses is focused on new regulation in data protection law. Theses analyses reasons why new regulation was enacted. It also analyses new duties and is focused on smaller controllers that have status of „public authority“. Theses also analyses contracts betwween processors and controllers and their impacts. The next objective of this is the data protection officer and its legal need for public authorities. It also examines if there is a need of wide definition of public authorities and contact between processor and controller. The last chapter is focused on the transfer of personal data to third-world countries.

Klíčová slova

GDPR, správce, pověřenec pro ochranu osobních údajů, zpracovatel

Key words

GDPR, controller, data protection officer, processor

Přílohy

OBEC CHROBOLY

Jak zasáhne GDPR Váš obecní rozpočet?

Implementace: 9000 bez DPH, měsíční platba: 600 Kč bez DPH

Jak jste řešili tzv. GAP analýzu GDPR (revizi osobních údajů)? V jaké cenové relaci byly nabídky?
Jakou jste vybrali a hodnotíte toto jako přínos?

Svaz místních samospráv ČR nabídl komplexní řešení problematiky spojené s GDPR. Finančně bezkonkurenční a vzhledem k tomu, že svaz byl založen k tomu, aby pomáhal především menším obcím, školám a školkám má nejvíce informací o všech činnostech, které se zde zajišťují. Jejich dosavadní spolupráci hodnotím jako přínos. Nabídky různých soukromých organizací, kterými jsou stále obce zavaleny jsou nesrovnatelně nákladnější a soustředí se povětšinou na to, jaké milionové sankce nám hrozí, jinak nic konkrétního. Některé nejagresivnější stále se opakující e-maily jsem musela nakonec zablokovat.

Jak ovlivní GDPR váš rozpočet? Na jakou částku implementace vyjde? Omezili jste kvůli tomu nějaké investice?

Cenu implementace jsem uvedla výše, žádné investice jsme omezovat nemuseli.Případné další náklady, kromě těch, co jsem napsala již na začátku, zatím nemohu odhadnout. Dle současných informací by GDPR nemělo celkový rozpočet nijak zvlášť ovlivnit. Pokud tedy nebude rozpočet čelit „MNOHAMILIONÉ SANKCI EURO“ , které by ho ovšem zruinovalo…

Jak jste se postavili k posouzení vlivu na ochranu osobních údajů? (Viz čl. 35 GDPR)

Ve spolupráci s pověřencem jsme zpracovali přehledné tabulky, ve kterých jsou uvedeny všechny agendy a rozsah zpracování osobních údajů pro každou zvlášť (nezpracováváme citlivé údaje). Neprovádíme žádný cílený monitoring osobních údajů, z povahy činnosti veřejné zprávy zpracováváme tyto údaje na základě zákona. Nejrozsáhlejší agenda je evidence osob hlášených k trvalému pobytu v obci, tyto údaje jsou získávány z centrálního registru obyvatel na základě zákona o evidenci obyvatelstva, vedeny jsou v elektronické formě v programu společnosti ALIS, spol. s r.o., přístup do tohoto programu je chráněn heslem. Pověřenec na základě těchto námi dodaných informací vyhodnotí míru rizika a stanoví postup pro případ incidentu. Všechny potřebné informace včetně kontaktu na pověřence budou v souladu se zákonem zveřejněny na webových stránkách obce.

Jak zabezpečujete údaje? Našli jste rozpor s GDPR po revizi? (Pokud jste ji již udělali)

Údaje v listinné podobě jsou uchovávány v uzamčených prostorách obecního úřadu, budova je opatřena alarmem, elektronické údaje jsou chráněny heslem, a to jak samotný přístup do počítačů, tak i do konkrétních programů, ve kterých se s osobními údaji pracuje. Žádný rozpor jsme neshledali.

Jak budete řešit funkci pověřence pro ochranu osobních údajů? (externě, současným zaměstnancem)? Jak je to pro vás finančně náročné?

Smluvně se Svazem místních samospráv. Finanční zatížení je uvedeno výše.

Pokud současným zaměstnancem, jakým způsobem jste ho proškolili?

…….

Jaké náklady na pověřence odhadujete ročně?

Viz výše.

Zpracováváte nějaké osobní údaje ze zahraničí? Jak je předáváte a jakým způsobem je budete chránit?

Nezpracováváme.

Byl nějaký problém s uzavřením mlčenlivostí mezi správcem (městem) a zpracovateli (např. IT dodavatelé), nebo byli naklonění spolupráci?

Nebyl žádný problém.

Bude mít implementace GDPR vliv smluvní dokumentaci a revize smluv ne/bude znamenat zvýšené náklady?

Zpracovatelé, což jsou IT firmy, které z titulu služeb, které poskytují, mají přístup do agend, ve kterých se zpracovávají osobní údaje, zaslali dodatek v souladu s GDPR. Revize smluv neznamená žádné zvýšené náklady.

Jak revize smluv postihne efektivitu obce a obecního úřadu? (Myslím např. v samostatné působnosti, jestli Vás takové opatření zdržuje od práce, v případě přenesené, jestli Vám poskytuje součinnost stát ať finančními prostředky nebo školením.)

Veškeré informace obsaženy v námi vyhotovených smlouvách obsahují pouze údaje potřebné pro uzavření těchto smluv, tedy údaje poskytnuté z titulu zákonnosti. Všechny povinnosti, stanovené GDPR budou splněny uveřejněním informací o zpracování osobních údajů na webových stránkách obce. Do nově uzavíraných smluv se navíc vloží pouze informace o tom, že podrobné informace o zpracování osobních údajů a kontakt na pověřence je zveřejněn na webových stránkách obce (vloží se hypertextový odkaz na umístění).

Myslíte si, že role státu v oblasti GDPR je/byla nedostatečná?

Role státu nebyla a není žádná. Alespoň dle mého názoru.

Vážený pane

kolem Nařízení EU o zavedení GDPR je stále spousta nejasností, názory odborníků na aplikaci ve veřejné správě se liší, takže na některé otázky Vám zatím nemohu konkrétně odpovědět.

- snažíme se o minimální zásah do rozpočtu města - jednorázově budou pořízeny aktualizace programů, u nichž nemáme servisní smlouvu, ostatní budou upraveny zdarma. Hradili jsme školení pracovníka MěÚ jako pověřence, další náklady budou s pořízením uzamykatelných skříní apod., tedy cca. 50.000,- Kč;

- GAP analýzu řešíme vlastními silami s pomocí metodiky MV. Obdrželi jsme jednu cenovou nabídku od externí firmy (měú za 40.000,- Kč, za 3 příspěvkové organizace po 15.000,- Kč);

- rozpočet města nebude GDPR ovlivněn, mírně se navýší rozpočet na správu (modernizujeme IT vybavení úřadu z dotace, bude vylepšeno zabezpečení sítě a zálohování našich informačních systémů), investice nebudou v žádném případě kvůli tomu omezeny;

- posouzení vlivu provádí proškolený pověřenec ve spolupráci s vedením úřadu s každým zaměstnancem;

- v současném zabezpečení byly shledány drobné rozpory, na jejich zabezpečení se pracuje;

- pověřencem bude současný zaměstnanec, kterému bude upraveno platové ohodnocení v souladu s katalogem prací;

- školení pověřence probíhá kombinovanou formou (3 dny školení + samostudium) se závěrečným testem u pražské odborné firmy;

- náklady na výkon pověřence - odhaduji na cca 30.000,- Kč ročně;

- údaje ze zahraničí nezpracováváme;

- bez problémů - smluvně ošetřeno již v minulosti podle z.č. 101/2000 Sb. + revize a aktualizace smluv;

- bude provedena revize a aktualizace smluv - zvýšené náklady na právní služby cca 30.000,- Kč;

- činnost úřadu nebude (nesmí být) negativně zasažena, je to však další zatěžující práce bez jasných pravidel a metodiky ... /tak jako se vším "lidová tvořivost"/

- role státu je naprosto nedostatečná, opět je ČR "papežštější než papež"!

OBEC KVILDA

datum: 20. května 2018 vyřizuje:

Vážený pan

Věc: Žádost o přístupu k informacím

Odpovědi na Vaše otázky:

- **pouze v rámci nákladů a nejsou omezeny další investice**
- **souhrnnou zprávu máme zpracovanou od firmy Keystone compeny a.s. za cenu 7.000,- Kč. (ostatní většinou kolem 10.000,- Kč.)**
- **po souhrnné zprávě GDPR vše napraveno**
- **pověřence zajistí též firma Keystone compeny a.s. za cenu 1.000,- Kč. měsíčně**
- **osobní údaje ze zahraničí nezpracováváme**
- **smlouvy o mlčenlivosti máme uzavřeny**
- **implementace GDPR nebude mít vliv na cenu smluvní dokumentace a revize smluv**
- **efektivitu obce a obecního úřadu GDPR jist postihne**
- **role státu v oblasti GDPR je přiměřená**

S pozdravem

starosta obce Kvilda

Jak zasáhne GDPR Váš obecní rozpočet? Pro rok 2018 cca 50000 Kč

Jak jste řešili tzv. GAP analýzu GDPR (revizi osobních údajů)? V jaké cenové relaci byly nabídky? Jakou jste vybrali a hodnotíte toto jako přínos? V relaci 30000 – 160000, pro Obec +ZŠ, vybrali jsme nejnižší

Jak ovlivní GDPR váš rozpočet? Na jakou částku implementace vyjde? Omezili jste kvůli tomu nějaké investice? V rozpočtu jsme s těmito výdaji počítali, žádné investice jsme neomezili.

Jak jste se postavili k posouzení vlivu na ochranu osobních údajů? (Viz čl. 35 GDPR) Zatím nevím

Jak zabezpečujete údaje? Našli jste rozpor s GDPR po revizi? (Pokud jste ji již udělali) Zatím nedělali

Jak budete řešit funkci pověřence pro ochranu osobních údajů? (externě, současným zaměstnancem)? Jak je to pro vás finančně náročné? Externě 1600 Kč/měsíčně

Pokud současným zaměstnancem, jakým způsobem jste ho proškolili?

Jaké náklady na pověřence odhadujete ročně? 20 000,-Kč

Zpracováváte nějaké osobní údaje ze zahraničí? Jak je předáváte a jakým způsobem je budete chránit? Nezpracováváme

Byl nějaký problém s uzavřením mlčenlivostí mezi správcem (městem) a zpracovateli (např. IT dodavatelé), nebo byli naklonění spolupráci? Nebyl

Bude mít implementace GDPR vliv smluvní dokumentaci a revize smluv ne/bude znamenat zvýšené náklady? Nevím, ukáže čas

Jak revize smluv postihne efektivitu obce a obecního úřadu? (Myslím např. v samostatné působnosti, jestli Vás takové opatření zdržuje od práce, v případě přenesené, jestli Vám poskytuje součinnost stát ať finančními prostředky nebo školením.) Uvidíme časem

Myslíte si, že role státu v oblasti GDPR je/byla nedostatečná? Myslím si, že byla nedostatečná

[redacted], starosta, Obec Lenora, Lenora 36

Obec Lenora

MĚSTO PÍSEK
KANCELÁŘ ÚŘADU
Velké náměstí 114/3, 397 19 Písek

Vážený pan

Č.j.: MUPI/2018/17858

V Písku 4. května 2018

Sdělení k žádosti o poskytnutí informace dle zákona č. 106/1999 Sb.

Dne 23.04.2018 byla na Městský úřad Písek doručena Vaše žádost dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, o poskytnutí níže uvedených informací. K jednotlivým dotazům uvádíme následující:

Jak zasáhne GDPR Váš obecní rozpočet?

V současné době nelze stanovit celkové náklady na implementaci GDPR. Dosud byla z rozpočtu hrazena GAP analýza a byl přijat nový zaměstnanec na pozici pověřence.

Jak jste řešili tzv. GAP analýzu GDPR (revizi osobních údajů)? V jaké cenové relaci byly nabídky? Jakou jste vybrali a hodnotíte toto jako přínos?

GAP analýza byla prováděna externím subjektem. Cenové nabídky se pohybovaly v rozmezí 175 až 250 tisíc Kč bez DPH. Byla vybrána nejnižší cenová nabídka. Analýza byla přínosem.

Jak ovlivní GDPR váš rozpočet? Na jakou částku implementace vyjde? Omezili jste kvůli tomu nějaké investice?

Zde odkazujeme na odpověď na první dotaz. Žádné investice nebyly v přímé souvislosti s GDPR omezovány.

Jak jste se postavili k posouzení vlivu na ochranu osobních údajů? (Viz čl. 35 GDPR)

U agend se silnou rizikovostí probíhají přípravné práce na vypracování posouzení vlivu. U agend, kde je zpracování osobních údajů dáno zákonem, je doporučeno vyčkat na schválení příslušného zákona.

Jak zabezpečujete údaje? Našli jste rozpor s GDPR po revizi? (Pokud jste ji již udělali)

Rozpory byly méně závažného charakteru. Provádí se organizační a technická opatření.

Jak budete řešit funkci pověřence pro ochranu osobních údajů? (externě, současným zaměstnancem)? Jak je to pro vás finančně náročné?

Funkce pověřence byla vyřešena přijetím nového zaměstnance. Celkovou finanční náročnost nelze v současné době ještě stanovit.

Pokud současným zaměstnancem, jakým způsobem jste ho proškolili?

Jedná se o nového zaměstnance a nikoliv současného.

Jaké náklady na pověřence odhadujete ročně?

Celkové finanční náklady nelze v současné době ještě stanovit.

Zpracováváte nějaké osobní údaje ze zahraničí? Jak je předáváte a jakým způsobem je budete chránit?

Nezpracováváme.

Byl nějaký problém s uzavřením mlčenlivostí mezi správcem (městem) a zpracovateli (např. IT dodavatelé), nebo byli naklonění spolupráci?

Zpracovatelské smlouvy se průběžně zpracovávají. Zatím nebyly zjištěny problémy.

Bude mít implementace GDPR vliv smluvní dokumentaci a revize smluv ne/bude znamenat zvýšené náklady?

Implementace GDPR vyžaduje menší úpravy ve smlouvách (informace o zpracování osobních údajů). Náklady nelze stanovit.

Jak revize smluv postihne efektivitu obce a obecního úřadu? (Myslím např. v samostatné působnosti, jestli Vás takové opatření zdržuje od práce, v případě přenesené, jestli Vám poskytuje součinnost stát ať finančními prostředky nebo školením.)

Nelze hodnotit.

Myslíte si, že role státu v oblasti GDPR je/byla nedostatečná?

Nelze hodnotit.

S pozdravem

MĚSTSKÝ ÚŘAD PÍSEK
KANCELÁŘ ÚŘADU

Mgr. Bc.
vedoucí odboru

OBEC HORNÍ VLTAVICE, 384 91 Horní Vltavice 80
tel. 388 436 303, 724 233 644, e-mail: info@hvltavice.cz

Č.j. ohvl- /2018

Horní Vltavice 4. 5. 2018

Žádost dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Jak zasáhne GDPR Váš obecní rozpočet? ***Nijak zásadně.***
Jak jste řešili tzv. GAP analýzu GDPR (revizi osobních údajů)? V jaké cenové relaci byly nabídky? Jakou jste vybrali a hodnotíte toto jako přínos? ***Analýza byla provedena vlastními silami.***
Jak ovlivní GDPR váš rozpočet? Na jakou částku implementace vyjde? Omezili jste kvůli tomu nějaké investice? ***GDPR neovlivní rozpočet ani investiční činnost obce.***
Jak jste se postavili k posouzení vlivu na ochranu osobních údajů? (Viz čl. 35 GDPR) ***Údaje dle článku 35 neevidujeme.***
Jak zabezpečujete údaje? Našli jste rozpor s GDPR po revizi? (Pokud jste ji již udělali)
Jak budete řešit funkci pověřence pro ochranu osobních údajů? (externě, současným zaměstnancem)? Jak je to pro vás finančně náročné? ***Externě, není finančně náročné.***
Pokud současným zaměstnancem, jakým způsobem jste ho proškolili? -
Jaké náklady na pověřence odhadujete ročně? ***Externí pracovník bude vykonávat zdarma.***
Zpracováváte nějaké osobní údaje ze zahraničí? Jak je předáváte a jakým způsobem je budete chránit? ***Nezpracováváme, pokud by k tomu došlo, tak stejným způsobem jako u osob. údajů občanů ČR.***
Byl nějaký problém s uzavřením mlčenlivostí mezi správcem (městem) a zpracovateli (např. IT dodavatelé), nebo byli naklonění spolupráci? ***Nenastal žádný problém, spolupráci byli nakloněni.***
Bude mít implementace GDPR vliv smluvní dokumentaci a revize smluv ne/bude znamenat zvýšené náklady? ***Nebude znamenat zvýšené náklady.***
Jak revize smluv postihne efektivitu obce a obecního úřadu? (Myslím např. v samostatné působnosti, jestli Vás takové opatření zdržuje od práce, v případě přenesené, jestli Vám poskytuje součinnost stát ať finančními prostředky nebo školením.) ***Efektivitu naší obce nepostihne.***
Myslíte si, že role státu v oblasti GDPR je/byla nedostatečná? ***Dostatečná, ale trochu opožděná.***

S pozdravem

starosta

Městys Strážný
384 43 STRÁŽNÝ 23

VÁŠ DOPIS:
ZE DNE: 24.4.2018
NAŠE ZN.: MSTR-461/2018

VYŘIZUJE:
TEL.: 388 437 128
E-MAIL: mestys@strazny.cz

DATUM: 24.4.2018

Poskytnutí informace v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím - GDPR

1. V této chvíli nevíme, jakou měrou zasáhne GDPR obecní rozpočet. Nemáme stanovenou cenu za pověřence.

2. Nechali jsme zpracovat od firmy za cenu 25 000,- Kč. Ostatní nabídky byly vyšší. Bez této firmy bychom nebyli schopni sami analýzu provést.

3. Viz. odst. 1 a 2. Investice jsme neomezili.

4. Analýzu obdržíme začátkem měsíce května 2018.

5. Revizi zatím nemáme.

6. Externě. Cena zatím není stanovena.

7. –

8. Nevím.

9. Údaje ze zahraničí nezpracováváme.

10. Spolupráce bez problémů.

11. Neumíme odhadnout.

12. Veškeré revize smluv nás budou zatěžovat.

13. Role státu v oblasti GDPR byla nedostatečná.

S pozdravem

Mgr.
starostka

MĚSTYS STRÁŽNÝ
384 43 Strážný 23
IČ 00250 694
DIČ CZ00250 694
mestys@strazny.cz
tel. 384 437 128