Ústecký kraj

Velká Hradební 3118/48
400 02 Ústí nad Labem

Věc: Stanovisko k aplikaci Nařízení GDPR

OBSAH:

1. Předmět stanoviska 2
2. Obecné principy aplikace GDPR 2
3. Zpracování osobních údajů poskytovateli sociálních služeb 3
4. Stávající situace PSS před účinností GDPR 4
5. Aplikace GDPR 4
6. Desatero základních povinností v oblasti ochrany osobních údajů 5
7. Vyhodnocení souladu s GDPR 5
8. Soubor opatření k zajištění souladu s GDPR 8
9. Povinnost jmenovat pověřence na ochranu osobních údajů 9
10. Náklady na zajištění souladu s GDPR 10
11. Uznatelnost nákladů na zajištění souladu s GDPR při krytí z veřejných zdrojů 10
12. Možnost zahrnutí nákladů na zajištění souladu s GDPR do vyrovnávací platby 11
13. Limity nákladů na zajištění souladu s GDPR 12
14. Uznatelnost nákladů na zajištění souladu s GDPR z pohledu dotačního programu 13
15. Závěr – shrnutí odpovědi na položené dotazy 14
16. Příloha - Služby k zajištění souladu s GDPR ..... **Chyba! Záložka není definována.**

1. Předmět stanoviska

1.1. Předmětem tohoto stanoviska je rozbor dopadů aplikace Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále pro účely tohoto stanoviska "***GDPR***"), a to zejména **na činnost poskytovatelů sociálních služeb v krajské síti Ústeckého kraje**.

1.2. Stanovisko je zaměřeno k zodpovězení dotazu poskytovatelů sociálních služeb v tomto znění:

(i) *Jaké mohou být jednorázové náklady poskytovatelů sociálních služeb při vstupu do systému GDPR a jaké mohou být další navazující, opakovatelné náklady a jak se mohou promítnout do uznatelných nákladů v rámci dotačního řízení „Podpora sociálních služeb v Ústeckém kraji", resp. následně do podmínek financování sociálních služeb?*

(ii) *Existují nějaké limity pro výši nákladů? Pokud je regulace stanovena či má být stanovena krajem, žádáme o vyjádření k limitům, zda je možné je zahrnout jako uznatelné náklady v rámci dotačního řízení?*

2. Obecné principy aplikace GDPR

2.1. Podle článku 99 GDPR se toto nařízení použije ode dne 25. 5. 2018.

2.2. GDPR se vztahuje na všechny subjekty, které zpracovávají osobní údaje fyzických osob, a to na **zcela nebo částečně automatizované zpracování osobních údajů a na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny**. Za evidenci GDPR považuje jakýkoliv strukturovaný soubor osobních údajů přístupných podle zvláštních kritérií, ať již je centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska.

2.3. **Za osobní údaje** GDPR považuje veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

2.4. GDPR definuje navíc tzv. zvláštní kategorie osobních údajů („***citlivé údaje***"), jejichž zpracování podléhá přísnějším kritériím a které podléhají zvýšené míře ochrany. Za citlivé údaje jsou považovány údaje, které vypovídají o rasovém či etnickém původu, politických

Z KLUB
Z klub s.r.o
Lužná794/17
160 00 Praha 6 – Vokovice
IČ: 24146463

Městský soud v Praze
oddíl C, vložka C 182924
E: info@zklub.cz,
W: www.zklub.cz

názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby.

2.5. **Zpracováním osobních údajů** GDPR rozumí jakoukoliv operaci nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

3. Zpracování osobních údajů poskytovateli sociálních služeb

3.1. Poskytovatelé sociálních služeb („***PSS***“) zpracovávají osobní údaje zejména následujících fyzických osob („***subjekty údajů***“):

(i) osoby, jimž jsou sociální služby a další navazující aktivity poskytovány („***klienti***“);

(ii) rodinní příslušníci klientů a další kontaktní a blízké osoby jednající s PSS v zájmu klienta, příznivci PSS apod.;

(iii) zaměstnanci PSS;

(iv) dobrovolníci vykonávající dobrovolnickou službu podle zákona č. 198/2002 Sb., o dobrovolnické službě, ve znění pozdějších předpisů;

(v) osoby samostatně výdělečně činné na pozici spolupracujících osob, dodavatelů, obchodních partnerů apod. včetně lékařů, advokátů, psychologů apod.;

(vi) zástupci a kontaktní osoby právnických osob – partnerů, dodavatelů, sponzorů, veřejných institucí, poskytovatelů dotací apod.;

(vii) návštěvníci zařízení sociálních služeb (evidence návštěv, kamerový systém).

3.2. Ze shora uvedeného důvodu jsou PSS považováni za tzv. **správce osobních údajů.**

3.3. Množství a kategorie zpracování osobních údajů u jednotlivých subjektů údajů je dána zejména účelem zpracování ve vztahu k právnímu titulu jejich zpracování. Zejména u klientů a zaměstnanců půjde zpravidla vždy o zpracování osobních údajů **včetně citlivých údajů.**

3.4. PSS zpracovávají osobní údaje u jednotlivých subjektů údajů v závislosti na časové fázi vztahu PSS k subjektu údajů. Každá fáze zpracování může být založena na jiném právním titulu a bude zpravidla vyžadovat též jiný nezbytný rozsah zpracování dle zásad účelového omezení a minimalizace zpracování osobních údajů.

3.5. U zpracování osobních údajů klientů lze zaznamenat zpravidla tuto časovou osu:

(i) fáze zájemce o službu (zjišťování situace a potřeb určité osoby);

(ii) fáze poskytování sociální služby (tato fáze může být členěna v závislosti na změně potřeb dle individuálního plánu klienta);

(iii) fáze v souvislosti s ukončením služby (ukončení služby, změna PSS nebo úmrtí klienta);

(iv) fáze po ukončení služby (uchovávání a archivace údajů, dodatečné služby pozůstalým atp.).

3.6. Obdobné časové fáze lze zaznamenat i ve vztahu k ostatním subjektům údajů (např. u zaměstnanců fáze NÁBOR – EVIDENCE UCHAZEČE – ZAMĚSTNANEC nebo ODMÍTNUTÝ UCHAZEČ – BÝVALÝ ZAMĚSTNANEC.

4. Stávající situace PSS před účinností GDPR

4.1. Aplikace GDPR ze strany PSS v žádném případě **neznamená zavedení zcela nových pravidel, která by PSS v současnosti neznali**. PSS jsou již dnes povinni plnit řadu povinností ve vztahu k ochraně osobních údajů, a to na základě stávající platné právní úpravy, kterou regulují zejména:

(i) zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů;

(ii) Směrnice EP a Rady 95/46/ES ze dne 14. 10. 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;

(iii) výkladová stanoviska Úřadu pro ochranu osobních údajů.

4.2. PSS mají v současné době zavedenu řadu standardů ochrany osobních údajů, ať již v podobě vnitřních předpisů, opatření technické či organizační povahy, režimu souhlasů se zpracováním osobních údajů, omezení přístupu osob k osobním údajům dle funkčního zařazení v organizaci, školení zaměstnanců, uzavřených smluv s dodavateli služeb atp.

4.3. Z uvedeného vyplývá, že aplikace GDPR neznamená ve svém důsledku pro PSS masivní zavedení nových standardů, ale spíše přizpůsobení a korekce zavedených standardů podle pravidel GDPR. V tomto ohledu nutno chápat i nezbytné náklady, které mohou být s aplikací GDPR ze strany PSS spojeny.

5. Aplikace GDPR

5.1. Právní regulace standardů ochrany osobních údajů, spojená se zaváděním GDPR v praxi, vychází zejména z následujících předpisů (a dokumentů metodické povahy):

(i) Nařízení GDPR;

(ii) připravovaný zákon o zpracování osobních údajů;

(iii) vodítka a pokyny Pracovní skupiny WP29;

(iv) https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=21750

(v) metodické materiály Úřadu pro ochranu OÚ(např. FAQ);

(vi) https://www.uoou.cz/gdpr/ds-3938/p1=3938

(vii) metodické doporučení MV obcím (např. https://www.gdpr.cz/gdpr/metodicke-doporuceni-k-cinnosti-obci-ministerstvo-vnitra/

6. Desatero základních povinností v oblasti ochrany osobních údajů

6.1. Přestože rozbor jednotlivých povinností dle GDPR není předmětem tohoto Stanoviska, je z důvodu provedení analýzy nákladů vhodné nastínit alespoň jejich základní přehled.

6.2. Oproti dosavadní právní úpravě ochrany osobních údajů opouští GDPR koncepci povinné oznamovací povinnosti zpracování osobních údajů vůči Úřadu pro ochranu osobních údajů; namísto toho zavádí pro správce osobních údajů povinnost **být schopen doložit soulad s GDPR**; PSS coby správce osobních údajů tak nese důkazní břemeno o tom, že plní všechny povinnosti v oblasti ochrany osobních údajů dle GDPR.

6.3. Základní povinnosti, které jsou PSS coby správci osobních údajů povinni dle GDPR dodržet, lze shrnout do jakéhosi **desatera**:

(i) prokázat soulad s GDPR, tj. naplňování dalších jednotlivých povinností (viz výše);

(ii) dodržovat zásady zpracování osobních údajů;

(iii) zavést vhodná technická a organizační opatření;

(iv) minimalizovat zpracování osobních údajů;

(v) informovat subjekty údajů o zpracování;

(vi) zajistit usnadnění výkonu práv subjektů údajů;

(vii) vést záznamy o činnostech zpracování;

(viii) ohlašovat a oznamovat případné bezpečnostní incidenty;

(ix) jmenovat pověřence pro ochranu osobních údajů (je-li jeho jmenování povinné);

(x) dle situace provést posouzení vlivu a projít předchozí konzultací s Úřadem na ochranu osobních údajů.

7. Vyhodnocení souladu s GDPR

7.1. Jak již bylo uvedeno výše, PSS jsou povinni zajistit soulad s GDPR do dne nabytí jeho účinnosti (tj. do 25. 5. 2018) a toto zajištění souladu být schopni prokázat.

7.2. Zajištění souladu předpokládá realizaci zejména následujících kroků:

(i) provedení posouzení (zmapování) stávající úrovně ochrany osobních údajů v organizaci;

(ii) provedení porovnání stávající úrovně ochrany s požadavky GDPR;

(iii) vyhodnocení rizik spojených se zpracováním osobních údajů;

(iv) přijetí a zavedení souboru opatření fyzické a IT ochrany k zajištění souladu, a to jednorázových, opakovaných a průběžných.

7.3. Každý PSS by měl v co nejbližší době **zmapovat své individuální v současnosti zavedené standardy ochrany osobních údajů**. Tato úvodní fáze spočívá zejména v tom, že PSS:

(i) zmapuje, jaké všechny osobní údaje zpracovává a jakých subjektů osobních údajů se týkají;

(ii) vymezí, které ze zpracovávaných osobních údajů spadají do zvláštní kategorie (tzv. citlivé údaje);

(iii) zreviduje účel, k jakému ty které osobní údaje získává / zpracovává;

(iv) určí právní titul, na základě kterého údaje zpracovává;

(v) vyhodnotí nezbytnost rozsahu zpracovávaných osobních údajů ve vztahu k časové fázi zpracování (viz body 3.5 a 3.6. výše)

(vi) vyhodnotí, kdo a za jakých podmínek má k osobním údajům přístup a jak jsou zajištěna rizika bezpečnostních událostí (ztráty, poškození, úniku, zneužití údajů);

(vii) vyhodnotí rizika dopadu případné bezpečnostní události na práva a svobody subjektů údajů.

7.3.1. Zmapování, jaké všechny osobní údaje PSS zpracovává, by měl PSS učinit vlastními silami, resp. za pomoci odborného aparátu, kterým disponuje a který nejlépe zná činnost organizace v oblasti zpracování osobních údajů. Jde o to nezapomenout na žádné údaje, byť jejich zpracování nemusí být na první pohled zjevné (např. fotografie, kamerové záznamy apod.).

7.3.2. PSS budou velmi často zpracovávat tzv. **citlivé údaje** (viz bod 2.4. výše) zejména ve vztahu ke klientům sociální služby. Je důležité mít tyto údaje velmi dobře zmapovány, neboť GDPR stojí na principu zvýšené ochrany těchto osobních údajů a zpřísnění povinností při jejich zpracování.

7.3.3. Zmapování účelu, tj. z jakého důvodu PSS osobní údaje získává, je velmi důležité pro naplnění zásady zákonnosti a zásady minimalizace zpracování údajů. Podle GDPR nemá PSS zpracovávat jakékoliv údaje, které nezbytně nepotřebuje ke své činnosti. Účel zpracování spoluurčuje právní titul, na základě kterého PSS může údaje zpracovávat.

7.3.4. Jak bylo výše uvedeno, účel zpracování koresponduje s právním titulem zpracování. GDPR na rozdíl od dosavadní právní úpravy zcela opouští koncepci souhlasu subjektu údajů se zpracováním jako základního právního titulu. Souhlas má být nadále vyžadován a používán výlučně tehdy, pokud PSS nesvědčí jiný právní titul. GDPR navíc přináší zpřísnění požadavků na získání souhlasu.

7.3.5. PSS budou proto nadále kromě souhlasu subjektu údajů využívat zejména následující právní tituly zpracování osobních údajů:

(i) zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů (např. smlouva o poskytování sociální služby);

(ii) zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce (např. PSS zařazený do krajské sítě, disponující Pověřením SGEI);

(iii) zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje (např. povinnosti plynoucí ze zákona o sociálních službách ve vztahu ke standardům, povinnosti archivace podle zákona či dotační smlouvy atd.);

(iv) zpracování je nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany (např. monitoring pohybu osob v zařízeních z důvodu ochrany majetku a bezpečnosti apod.).

7.3.6. V rámci jednotlivých časových fází zpracování se jak účel zpracování, tak i právní titul zpravidla mění; tím je mnohdy dána i nezbytná změna (omezení) rozsahu zpracovávaných údajů. Splnění této povinnosti vyžaduje vstupní revizi a průběžný monitoring.

7.3.7. PSS musí zmapovat, kdo a za jakých podmínek má ke zpracovávaným osobním údajům přístup, a podle toho nastavit příslušná bezpečnostní opatření k eliminaci rizik vzniku bezpečnostních událostí.

7.3.8. Přístup k osobním údajům mají u PSS zpravidla následující osoby:

(i) členové statutárních a dalších orgánů;

(ii) zaměstnanci;

(iii) kontrolní orgány;

(iv) správci IT systémů;

(v) dodavatelé služeb mzdové a účetní agendy, finančního a daňového poradenství apod.

7.3.9. Pokud některé z výše uvedených osob kromě přístupu k osobním údajů provádějí též zpracování osobních údajů, jsou považovány podle GDPR za tzv. zpracovatele osobních údajů.

7.4. V návaznosti na zmapování stavu ochrany osobních údajů v organizaci musí PSS provést porovnání tohoto stavu s požadavky GDPR a vyhodnotit rizika zjištěného nesouladu. Vyhodnocení rizik je vhodné provést např. na stupnici:

(i) zanedbatelné;

(ii) malé;

(iii) střední;

(iv) vysoké.

7.5. Každému riziku je pak přiřazena adekvátní potřebná míra zásahu do stávajících standardů ochrany (přijetí nezbytných opatření), aby byl zajištěn soulad s GDPR.

8. Soubor opatření k zajištění souladu s GDPR

8.1. Zajištění souladu PSS s GDPR je založeno zejména na přijetí vhodných a ve vztahu k míře existujících rizik přiměřených opatření. Opatření lze v zásadě rozdělit na:

(i) opatření technické povahy;

(ii) opatření organizační a personální povahy;

(iii) opatření právní povahy.

8.2. Každé z výše uvedených opatření pak lze realizovat v oblasti zabezpečení elektronického zpracování osobních údajů (IT) a v oblasti zabezpečení fyzického zpracování osobních údajů (evidence).

8.3. Za opatření technické povahy lze považovat zejména:

(i) fyzická ochrana úložišť osobních údajů – zámky, mříže, centrální pult ochrany, elektronické zabezpečení, kamerový systém, kódovaný přístup apod.

(ii) ochrana úložišť osobních údajů na úrovni IT – bezpečnostní zálohy, šifrování, pseudonymizace, antivirová ochrana, aktualizace přístupových hesel apod.

8.4. Za opatření organizační a personální povahy lze považovat zejména:

(i) ochrana přístupu k osobním údajům podle funkčního principu;

(ii) systémové řešení ochrany osobních údajů v rámci organizačního schématu organizace (odpovědnost konkrétních pozic za ochranu dat, jmenování pověřence na ochranu osobních údajů apod.);

(iii) školení zaměstnanců;

(iv) zajištění funkční informační platformy vůči subjektům údajů apod.

8.5. Za opatření právní povahy lze považovat zejména:

(i) zpracování, resp. úprava existujících vnitřních předpisů a další dokumentace k ochraně osobních údajů a k usnadnění výkonu práv subjektů údajů;

(ii) úprava smluvních povinností ve smlouvách uzavřených se zaměstnanci, klienty, poradci, správci IT, dodavateli (mlčenlivost, prevence vzniku bezpečnostních událostí);

(iii) úprava smluv o zpracování osobních údajů se zpracovateli (např. externí zajištění účetní, mzdové agendy, daňové poradenství apod.;

(iv) průkazné vedení záznamů o zpracování osobních údajů;

(v) akceptace případně existujícího kodexu chování PSS;

(vi) případné získání osvědčení o souladu s GDPR ze strany akreditovaného subjektu.

9. Povinnost jmenovat pověřence na ochranu osobních údajů

9.1. Povinné zřízené funkce resp. jmenování tzv. pověřence pro ochranu osobních údajů upravuje článek 37 odst. 1 Nařízení GDPR v případě že,

- zpracování údajů provádí **orgán veřejné moci či veřejný subjekt** (s výjimkou soudů jednajících v rámci svých soudních pravomocí), nebo
- hlavní činnosti subjektu spočívají v operacích zpracování, které vyžadují rozsáhlé pravidelné a systematické monitorování subjektů údajů, a nebo
- hlavní činnosti subjektu spočívají v **rozsáhlém zpracování zvláštních kategorií údajů** a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

9.2. Pro určení, zda konkrétní PSS bude muset jmenovat pověřence, či nikoli, je na základě výše uvedených definic rozhodující zejména to, **zda jeho monitorování subjektů údajů lze označit za rozsáhlé, resp. zda jeho činnost spočívá v rozsáhlém zpracování citlivých údajů**.

9.3. Je-li PSS v postavení **organizační složky obce**, tj. orgánu veřejné moci, bude muset pověřence jmenovat již z titulu své právní formy. U **příspěvkových organizací** není prozatím v době vydání tohoto Stanoviska výkladově zcela vyjasněno, zda tuto právní formu nutno považovat za orgán veřejné moci resp. veřejný subjekt[1] či nikoli (objevují se odlišné právní názory).

9.4. Pojem „rozsáhlosti“ podle čl. 37 odst. 1 písm. b) a c) Nařízení GDPR je pojat obecněji, kdy při jeho zkoumání nutno zohlednit zejména počet subjektů údajů, kterých se zpracování údajů týká, objem zpracovávaných údajů, dobu nebo permanenci aktivit zpracování údajů, geografický rozsah aktivit zpracování údajů apod. Mezi příklady rozsáhlosti zpracování údajů je opět zahrnut příklad zpracování osobní údajů pacientů v nemocnicích na regionální úrovni apod.

9.5. Rozhodně ne každý PSS naplní definici rozsáhlosti monitorování subjektů údajů resp. rozsáhlosti zpracování citlivých osobních údajů. Proto ne každý PSS bude nucen jmenovat

[1] Viz důvodová zpráva k návrhu nového zákona na ochranu osobních údajů: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=KORNAQCDZPW5&tab=detail

pověřence. **Bližší definice pojmu „rozsáhlost“ s ohledem na počet subjektů údajů by snad měla být ještě vydána.**

10. Náklady na zajištění souladu s GDPR

10.1. V souvislosti s povinnou aplikací GDPR vzniknou PSS náklady, které budou muset vynaložit na zajištění souladu s GDPR. Lze předpokládat, že vesměs u všech PSS vzniknou náklady typově velmi podobné, a to:

(i) vstupní jednorázové náklady na zmapování současného stavu úrovně zajištění ochrany osobních údajů;

(ii) vstupní jednorázové náklady na identifikaci nesouladu s GDPR a zhodnocení rizik;

(iii) vstupní jednorázové náklady na přijetí souboru opatření uvedených v bodě 8. výše k zajištění souladu s GDPR;

(iv) náklady na průběžnou, resp. opakovanou aktualizaci opatření k prokázání souladu s GDPR;

(v) průběžné náklady na osobu pověřence (interního zaměstnance nebo externího dodavatele);

(vi) případné opakované náklady na získání osvědčení o souladu od akreditovaného subjektu (osvědčení se má udělovat na 3 roky).

10.2. Výše jednotlivých nákladů však bude velmi individuální a bude odvislá zejména od:

(i) počtu subjektů údajů, jejichž údaje konkrétní PSS zpracovává;

(ii) výchozí úrovně standardů ochrany osobních údajů u PSS;

(iii) schopnosti PSS učinit některé kroky k zajištění souladu s GDPR vlastními silami (stávajícími odbornými pracovníky).

10.3. Z rešerše současné nabídky služeb v souvislosti se zaváděním standardů dle GDPR na relevantním trhu lze předpokládat velmi rozdílnou úroveň nákladů. Vstupní náklady na zajištění souladu se pohybují v závislosti na množství subjektů údajů, organizační struktuře a velikosti organizace a předmětu činnosti organizace v rozmezí 30 – 150 tisíc Kč. Náklady na pověřence osobních údajů pak od 1.500,- Kč do 12.000,- Kč měsíčně.

11. Uznatelnost nákladů na zajištění souladu s GDPR při krytí z veřejných zdrojů

11.1. Uznatelnost krytí nákladů z veřejných zdrojů je v zásadě podmíněna splněním dvou podmínek:

(i) vynaložení nákladů naplňuje zásady hospodárnosti, účelnosti a efektivnosti; a

(ii) krytí nákladů nezakládá nedovolenou veřejnou podporu.

11.2. Pokud jde o otázku účelnosti nákladů, ta souvisí s otázkou jejich nezbytností; v zásadě lze konstatovat, že **náklady spojené se zajištěním souladu s GDPR bude možno považovat za nezbytné**, neboť jejich vynaložení vyplývá z plnění povinností stanovených zákonem a bez jejichž vynaložení nelze sociální služby řádně poskytovat.

11.3. **Naplnění zásad 3E** bude zajištěno zejména tím, že PSS zvolí takovou cestu implementace pravidel GDPR, která bude pro něj co nejefektivnější a bude učiněna za tržních (hospodárných) podmínek; přitom bude nutno zohlednit, zda a jak svými vlastními kapacitami mohl k danému cíli přispět.

11.4. Aby krytí nákladů na zajištění souladu s GDPR nezakládalo nedovolenou veřejnou podporu, musí být zajištěno splnění některé z následujících podmínek:

(i) PSS zpracovává osobní údaje výlučně v rámci činností, jejichž financování z veřejných zdrojů nezakládá veřejnou podporu podle článku 107 odst. 1 Smlouvy i fungování EU; takovým případem bude zpracování osobních údajů v rámci nehospodářské činnosti PSS, v rámci činností, které nemají potenciální dopad na hospodářskou soutěž ani na obchod mezi členskými státy EU), a/nebo

(ii) PSS zpracovává osobní údaje výlučně v rámci činností, jejichž financování z veřejných zdrojů zakládá veřejnou podporu slučitelnou s vnitřním trhem EU; takovým případem bude zpracování osobních údajů v rámci činností, které jsou kryty vyrovnávací platbou.

11.5. Pokud však PSS zpracovává osobní údaje i v rámci jiných činností, zejména těch, které mají hospodářskou povahu (pronájmy, doplňková či vedlejší hospodářská činnost PSS, určité druhy sociálního podnikání), hrozí riziko, že krytí takových nákladů na zajištění souladu s GDPR by mohlo představovat nedovolenou veřejnou podporu. V takovém případě mohou být náklady na zajištění souladu s GDPR poskytnuty PSS pouze:

(i) v rámci podpory malého rozsahu (*de minimis*); nebo

(ii) PSS musí zajistit pomocí vhodných nástrojů analytického účetnictví, že mu bude z veřejných zdrojů poskytnuto krytí pouze takové části nákladů na zajištění souladu s GDPR, která na základě vhodně zvolené metody alokace odpovídá nákladům na zajištění souladu s GDPR ve vztahu k činnostem, u nichž nehrozí riziko nedovolené veřejné podpory. Obdobný princip se aplikuje u vyrovnávací platby (viz dále bod 12.).

12. Možnost zahrnutí nákladů na zajištění souladu s GDPR do vyrovnávací platby

12.1. Na problematiku uznatelnosti nákladů vynaložených PSS na zajištění souladu s GDPR **v rámci vyrovnávací platby** nutno pohlížet očima Rozhodnutí Komise ze dne 20. 12. 2011 o použití čl. 106 odst. 2 Smlouvy o fungování Evropské unie na státní podporu ve formě vyrovnávací platby za závazek veřejné služby udělené určitým podnikům pověřeným

poskytování služeb obecného hospodářského zájmu (2012/21/EU, Úř. věst. L 7, 11. 1. 2012) – „***Rozhodnutí SGEI***“.

12.1.1. Podle článku 5 odst. 3 Rozhodnutí SGEI zahrnují náklady, k nimž se při stanovení vyrovnávací platby přihlíží, *„veškeré náklady vzniklé při poskytování služby obecného hospodářského zájmu. Vypočítají se na základě obecně přijatých zásad analytického účetnictví takto:*

a) vykonává-li dotčený podnik pouze činnosti v rozsahu služby obecného hospodářského zájmu, lze zohlednit jeho veškeré náklady;

b) vykonává-li dotčený podnik rovněž činnosti mimo rozsah služby obecného hospodářského zájmu, lze zohlednit pouze náklady vztahující se na poskytování služby obecného hospodářského zájmu;

c) náklady připisované službě obecného hospodářského zájmu mohou zahrnovat veškeré přímé náklady vynaložené při poskytování služby obecného hospodářského zájmu a odpovídající podíl nákladů společných službě obecného hospodářského zájmu a jiným činnostem“.

12.1.2. Z výše uvedeného principu uplatnění nákladů, resp. jejich alokované části v rámci vyrovnávací platby potom vyplývá, že u každého PSS bude situace odlišná a **bude závist na tom, ve vztahu k jakým činnostem PSS osobní údaje zpracovává.** Pokud bude PSS zpracovávat osobní údaje pouze ve vztahu k jedné sociální službě, bude možno zahrnout nezbytné náklady vynaložené na zajištění souladu s GDPR do vyrovnávací platby na danou sociální službu. Pokud se budou osobní údaje vázat k více sociálním službám, bude nutno náklady alokovat v příslušném poměru mezi všechny tyto služby. PSS v tomto případě bude postupovat obdobně, jako u jiných „společných“ nákladů na více služeb.

13. Limity nákladů na zajištění souladu s GDPR

13.1. Z výše uvedených zásad uznatelnosti nákladů na zajištění souladu s GDPR lze dovodit následující závěry:

(i) obecně z právních předpisů **nelze dovodit žádný „nepřekročitelný limit“ nákladů**, které lze hradit z veřejných zdrojů; náklady budou individuální pro jednotlivé PSS v závislosti na jejich úrovni současných standardů ochrany osobních údajů, velikosti, počtu subjektů údajů, druhu poskytované sociální služby apod.

(ii) v pohledu dotačního financování lze z veřejných zdrojů krýt pouze náklady, které jsou vynaloženy v souladu se zásadami 3E, tedy **účelně, hospodárně a efektivně**;

(iii) financování nákladů na zajištění souladu s GDPR z veřejných zdrojů nesmí představovat nedovolenou veřejnou podporu; výše míry intenzity podpory celkových nákladů musí být odvozena vždy od správné alokace příslušné části nákladů ke konkrétní činnosti PSS.

14. Uznatelnost nákladů na zajištění souladu s GDPR z pohledu dotačního programu

14.1. Finanční podpora na základě Dotačního programu „Podpora sociálních služeb v Ústeckém kraji 2018“ („***Program***“) je poskytována v režimu veřejné podpory slučitelné s vnitřním trhem podle Rozhodnutí SGEI. Subjekty, jejichž sociální služby jsou součástí Základní sítě kraje, obdrží či obdržely od Ústeckého kraje **Pověření Ústeckého kraje** k zajištění dostupnosti poskytování sociální služby zařazené do Základní sítě sociálních služeb Ústeckého kraje na období 2016–2018, které obsahuje, mimo jiné, kalkulaci maximální výše vyrovnávací platby. Míra podpory se řídí Principy a prioritami dotačního řízení na podporu poskytování sociálních služeb, které každoročně definuje MPSV, a Metodikou Ústeckého kraje pro poskytování finanční podpory poskytovatelům sociálních služeb v rámci programu Podpora sociálních služeb v Ústeckém kraji 2018 („***Metodika***“).

14.2. Podle části IV. Metodiky (zejm. body 13 – 20) a Přílohy č. 6 Metodiky jsou vymezeny tzv. uznatelné a neuznatelné náklady pro čerpání dotace poskytovatelům sociálních služeb. Obecně smí příjemce dotační prostředky použít pouze na úhradu nákladů na poskytování základních druhů a forem sociálních služeb v rozsahu stanoveném základními činnostmi při poskytování sociálních služeb pro příslušný druh sociální služby. Finanční prostředky z dotace lze čerpat pouze na výdaje časově a věcně související s kalendářním rokem, na který je dotace poskytnuta. Finanční prostředky pak nelze čerpat na uvedené tzv. „neuznatelné výdaje“, stanovené obecně článkem IV. bod 18 Metodiky a dále konkrétně v Příloze č. 6.

14.3. Pokud jde o posouzení nákladů vynaložených na zajištění souladu s GDPR, podle Metodiky **není možné z dotace hradit**:

(i) výdaje nesouvisející s poskytováním základních činností u jednotlivých druhů sociálních služeb; v tomto případě půjde o výše zmiňovaný případ, kdy zajištění souladu PSS s GDPR může zahrnovat i řadu dalších aktivit PSS nad rámec základních činností (hrazena by mohla být pouze alikvótní část takových nákladů přiřazených k základním činnostem na základě metod vedení analytického účetnictví);

(ii) zpracování auditů včetně auditu kvality; zde lze uvažovat o tom, že do této kategorie spadá i provedení jednorázového vstupního auditu souladu/nesouladu s GDPR, stejně tak náklady na získání osvědčení souladu s GDPR;

(iii) zpracování analýz, studií apod.; tato formulace opět svědčí o neuznatelnosti nákladů na jakoukoli vstupní analýzu souladu s GDPR, či analýzu standardů ochrany osobních údajů zavedených u PSSC apod.

14.4. Za **uznatelné náklady** by bylo možno považovat:

(i) konzultační, poradenské a právní služby související se zajištěním souladu s GDPR;

(ii) mzdu resp. část mzdy či odměny pověřence (pokud bude nutný);

(iii) služby – školení (vzdělávání pracovníků v oblasti GDPR).

ve všech případech však za dodržení základní podmínky dle bodu 14.3. (i) výše, tj. prokazatelné vazby výlučně za základní činnosti (tj. pouze určitá část alokovaných nákladů).

15. Závěr – shrnutí odpovědi na položené dotazy

15.1. **Otázka:** *Jaké mohou být jednorázové náklady poskytovatelů sociálních služeb při vstupu do systému GDPR a jaké mohou být další navazující, opakovatelné náklady a jak se mohou promítnout do uznatelných nákladů v rámci dotačního řízení „Podpora sociálních služeb v Ústeckém kraji“, resp. následně do podmínek financování sociálních služeb?*

15.1.1. **Odpověď:** Druhy nákladů spojených se zavedením souladu s GPR jsou specifikovány v bodě 10.1. tohoto Stanoviska. Výše jednotlivých nákladů bude zcela závislá na PSS – jeho velikosti, počtu subjektů údajů, druhu služby a dalších specifických podmínkách. Zjištěná výše některých nákladů z dostupných zdrojů je uvedena v bodě 10.3. Stanoviska. Současně nastavený Dotační program Podpora sociálních služeb v Ústeckém kraji umožňuje v rámci uznatelných nákladů financovat z dotace pouze náklady mzdové nebo náklady na externí konzultační, právní a poradenské služby, nebo vzdělávání, avšak za předpokladu, že tyto náklady jsou vynaloženy výlučně ve vztahu k základním činnostem poskytovaných sociálních služeb. Ochrana osobních údajů se týká jak základních činností, tak může v některých případech zasahovat i do činností dalších. Proto bude zpravidla možné hradit z dotace pouze alikvótní podíl celkových nákladů připadající na konkrétní službu a její základní činnosti.

15.2. **Otázka:** *Existují nějaké limity pro výši nákladů? Pokud je regulace stanovena či má být stanovena krajem, žádáme o vyjádření k limitům, zda je možné je zahrnout jako uznatelné náklady v rámci dotačního řízení?*

15.2.1. **Odpověď:** Žádné fixní limity výše nákladů neexistují, uznatelnost takových nákladů se bude řídit mj. zásadami efektivnosti, opodstatněnosti, hospodárnosti a věrohodnosti, jak vyplývá z Metodiky. S ohledem na **uznatelnost pouze příslušné účetně alokované části**

nákladů ve vazbě na základní činnosti, lze uvažovat o limitu stanoveném krajem, který by představoval:

(i) paušální příspěvek na poradenské služby v souvislosti se zajištěním souladu s GDPR (např. obdobně jako u účetního auditu);

(ii) paušální příspěvek na získání Osvědčení o souladu s GDPR od akreditované instituce (zatím nejsou stanoveny podmínky akreditace, ani cenová hladina);

(iii) příspěvek na mzdu, resp. odměnu pověřence, bude-li pro PSS tato pozice nezbytná;

(iv) příspěvek na vzdělávání pracovníků v oblasti GDPR.

V případě potřeby jsem připraven poskytnout další konzultační služby v této problematice.

V Praze dne 28. 11. 2017

JUDr. Karel Zuska