RELSIE spol. s r. o.
Na Valentince 644/15, 151 34 Praha 5

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Zpráva

ČÁST D2 – Varianty zajištění IT služeb

verze 2

k projektu

„Zajištění analýzy potřeb ÚMČ Praha 10 pro oblast ICT“

vypracovaná pro:

Městská část Praha 10

Zpracoval: kolektiv **RELSIE spol. s r. o**.

Sestavil: Houžvička

V Praze dne 17.9.2015 ……

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

1 OBSAH

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

2 MANAŽERSKÉ SHRNUTÍ

V této části je provedeno rychlé shrnutí výsledků a definováno doporučení dalšího postupu. Změny a úpravy této zprávy byly realizovány na základě projednaného stanoviska s jednotlivými politickými kluby. Na těchto jednáních bylo dosaženo konsensu, spolu se zástupci těchto klubů, o principech zajištění ICT potřeb úřadu a způsobu konstrukce jednotlivých variant.

V následující tabulce je uvedeno finanční porovnání jednotlivých variant definovaných v kap. 7, 8 a 9.

Ceny uváděny v Kč včetně DPH (zaokrouhleně).

	Var1	Var2	Var3
Cena	147,5mil	156,0mil	200,1mil.

Kde:

- Var1 – outsourcing v širší míře než aktuální (**bez tiskových služeb a Call Centra**)
- Var2 – outsourcing ve stejné míře jako aktuální (**bez tiskových služeb a Call Centra**) + části vlastními silami
- Var3 – interní provoz (**bez tiskových služeb a Call Centra**)

Kromě finančního hlediska je při volbě optimální varianty třeba zohlednit i existující rizika tak, jak jsou uvedena v kapitole č. 10.7.5.

Tato rizika nejsou výhradně personální (zabezpečení nového personálu, minimalizace jeho fluktuace, udržování jeho odborné úrovně, jeho řízení), ale i rizika spojená s výpadkem služby či rizika plynoucí z nedodržení platné legislativy, zejména v oblasti bezpečnosti systémů a ochrany osobních údajů.

Významným rizikem je i souběh více veřejných zakázek, jejichž plnění jsou na sobě závislá. Není možno garantovat, že soutěže, a z nich vyplývající smluvní vztahy, doběhnou podle časového plánu, nebo že některá ze soutěží nebude např. zrušena na základě rozhodnutí ÚOHS.

Varianta 1 může (při vhodném nastavení parametrů SLA) umožnit pružnější zavádění nových služeb a implementaci nové legislativy (evropská nařízení/směrnice o elektronické identitě, ochraně osobních údajů a kybernetické bezpečnosti, apod.).

Varianta 3 vytváří nová pracovní místa v dané lokalitě.

Je třeba zvážit rizika spojená s:

- s náborem a finančním ohodnocením nových pracovníků
- garancí odborné způsobilosti nových pracovníků
- přípravou pracovního prostředí a náplní práce nových pracovníků
- požadavky na fix time (oprava poruchy/výpadku) v řádu hodin u konkrétních systémů

Dalšími významnými riziky pro interní provoz (Var3) jsou:

- financování jednorázové obnovy spojené s architekturou a nasazením nových zařízení
- řízení dodavatelsko – odběratelských vztahů včetně řízení Help Desku
- dodržení požadovaných parametrů služeb ICT

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Rizika se obvykle lépe minimalizují prostřednictvím smluvního vztahu s příslušnými zárukami/sankcemi a vhodným rozdělením služeb tak, aby úřad mohl v budoucnu pružně využívat služby nabízené magistrátem, státem, případně jinými MČ, pokud to pro něj bude výhodné. To znamená, že úřad bude sledovat strategické vize a strategický rozvoj ICT v souladu s celopražskou koncepcí celopražských služeb a bude mít smlouvy koncipované tak, aby byl schopen flexibilně reagovat na nastalou situaci. Viz vyjádření MHMP v příloze č. 1. Konkrétní návrhy budou součástí výstupu části 3 projektu (RfP).

Doporučení v rámci tohoto projektu:

Pokračovat dále rozpracováním RfP dle rozhodnutí úřadu se zvláštním důrazem na strukturu a rozsah poptávaných služeb, jejich parametrů, způsobu kontroly a možnosti předčasného ukončení poskytování jednotlivých služeb.

Doporučení mimo tento projekt:

Zavést systém řízení ICT služeb na základě obecně uznávaných standardů a tento systém řízení jakosti služeb (ITSM) vyžadovat i od poskytovatele outsourcingu, včetně možnosti auditu poskytovatele třetí stranou.
To znamená, že by úřad měl mít možnost kontroly systému řízení jakosti služeb u poskytovatele outsourcingu a v **odůvodněných případech** tuto kontrolu provádět. Jedná se o jeden ze základních kontrolních mechanismů.

Zavedení řízení kvality služeb je nezbytné implementovat bez ohledu na to, zda jde o služby poskytované interně nebo externě. Pro tyto služby je tedy nezbytné definovat:

- Technické parametry (diskový prostor, výpočetní výkon, propustnost sítě, rizika, max. dobu odstávky atd. a to i v případě, že služby budou poskytovány MHMP nebo jinou pražskou částí)
- Personální parametry (včetně metodiky jak je počítána cena na pracovní místo)
- Legislativní požadavky (zejména požadavky zákona č. **101/2000Sb**. V aktuálním znění – uzavření příslušných smluv s externími subjekty, kterými jsou i MHMP nebo jiná pražská část i dle doporučení firmy Microsoft http://www.microsoft.com/enterprise/cs-cz/verejna-sprava/statni-sprava.aspx#fbid=ouHjHVSa78g, viz Příloha č. 2.

Další možnosti, např. využití veřejných cloud řešení, naráží na některá významná omezení:

- Osobní a citlivé údaje nesmí opustit území EU
- Velmi obtížně lze, u těchto řešení, zjistit kde se data aktuálně nachází a to především jejich kopie či zálohy. Tyto požadavky je třeba řešit smluvně.
- Firmy USA se musí řídit legislativou USA bez ohledu na to, v jakém státě podnikají, čímž vzniká významné riziko porušení naší legislativy http://www.reuters.com/article/2014/07/31/us-usa-tech-warrants-idUSKBN0G024I20140731?feedType=RSS viz příloha č. 3 a dále

  https://www.eff.org/files/2014/06/12/att_amicus_brief_in_support_of_microsoft_re_extraterritorial_search_warrant.pdf) viz Příloha č. 4

- SLA je prefabrikováno a poskytovatel obvykle nepřipustí změny, které by zvyšovaly jeho odpovědnost za cokoliv včetně ochrany dat.

Z tohoto pohledu se jako mnohem bezpečnější jeví využívání služeb vládního cloudu (gcloud) o jehož vzniku se uvažuje, případně využití služeb datového centra zpravovaného státním orgánem (SPCSS či odštěpný závod ČP).

Na základě porovnání uvedených variant lze pro zajištění vybraných ICT služeb úřadu vyhodnotit pokračování plného outsourcingu jako optimální cestu s minimálními riziky.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Akceptovatelným se jeví rovněž outsourcing klíčových služeb a soutěže na vybrané služby s minimální vazbou na služby klíčové. Jako klíčové služby chápeme aktiva s fix time v rámci hodin, jak jsou uvedena v tabulce v rámci kapitoly 6. Je však třeba vzít úvahu rizika popsaná výše.

Finální rozhodnutí je závislé na míře rizika a nárocích na pracovní místa, která bude třeba na úřadě vytvořit. Podstatnou roli i hraje i finanční aspekt, je třeba upozornit, že ve všech případech nelze předem odhadnout, jaké ceny budou ve vlastní soutěži dosaženy.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

3 POUŽÍVANÉ POJMY A ZKRATKY

DB	databáze
Fix time	doba do úplného odstranění poruchy/závady
FT	čas odstranění/opravy, doba od zahájení řešení události do jejího vyřešení
FTE	Full Time Equivalent (pracovní čas přepočítaný na plný úvazek)
HA	High Availability – vysoká dostupnost
HW	hardware
ISMS	Systém řízení bezpečnosti informací
ISVS	informační systémy veřejné správy ve smyslu zákona č. 365/2000 Sb. a návazných vyhlášek č. 529/2006 Sb. a č. 53/2007 Sb.
IT/ICT	informační technologie / informační komunikační technologie
ITSM	systém řízení jakosti služeb v IT/ICT
LAN	lokální datová síť
MČ P10	Městská část Praha 10
NAS	síťové úložiště dat
OIN	Odbor Informatiky
OS	operační systém
OVS	orgán veřejné správy
RfP	Request for proposal (žádost o nabídku)
RT	čas odezvy, doba od nahlášení události do doby potvrzení o zahájení řešení události (Response time)
SMS	systém managementu služeb úřadu
SW	Software

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

4 PŘEDMĚT PLNĚNÍ

Předmět plnění je definován následujícím textem:

„Na základě akceptovaného plnění D1 vyhotoví uchazeč varianty zajištění IT služeb zadavatele a to s ohledem na způsob zajišťování těchto služeb – interními zdroji, externími zdroji po oblastech, externími zdroji pomocí dominantních strategických partnerů. Součástí plnění bude doporučené „balíčkování“ služeb – rozdělení do věcných celků, které je vhodné zajišťovat společně (a to bez ohledu na to, že více balíků služeb může být nakonec zadáno jednomu Poskytovateli služeb).

Uchazeč vyhotoví rozhodovací podklady pro zadavatele, které budou obsahovat stručné shrnutí výhod a nevýhod jednotlivých variant ve vzájemném srovnání a základní propočet nákladů a jejich srovnání.

Zadavatel pro tyto účely poskytne základní finanční ukazatele relevantní pro vyhotovení takové srovnávací analýzy.

Dodavatel zohlední v doporučeném rozdělení celoměstské koncepce IT.“

Na základě zjištěných informací v části 1 projektu a rozhodnutí zadavatele jsou zpracovány tři varianty zajištění IT služeb.

4.1 PŘEDANÉ DOKUMENTY

Pro potřeby této zprávy by zpřístupněny smlouvy pro následující oblasti činností:

- Dodávky cartridgí a tonerů pro tiskárny ÚMČ Praha 10
- Údržba a služby pro zabezpečení provozu dodaného díla "Interaktivní úřední deska" (HW i SW)
- Smlouva o pronájmu diskového prostoru a poskytování souvisejících služeb
- Smlouva o poskytování služeb elektronických komunikací -internet
- Smlouva o poskytování odborného servisu
- Smlouva o poskytování elektronických komunikací - server housing
- Smlouva o technickém zajištění obsluhy systémů
- Smlouva o poskytování služby Webcall
- Rámcová smlouva - dodatek
- Smlouva o nájmu multifunkčních zařízení a souvisejících služeb
- Smlouva zajištění běžného provozu a rozvoje portálů a dalších webových presentací MČ Praha 10
- Smlouva o poskytování služeb provozu webových presentací Prahy 10 - servisní smlouva

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

5 ŘÍZENÍ INFORMATIKY ÚŘADU

Při posuzování problematiky outsourcingu ICT úřadu lze pohlížet na oblast informatiky úřadu, tj. provoz požadovaných IS a s nimi související IT technologií (bez ohledu na to, jakým způsobem je zajišťován jejich činnost) jako na jednotku (či oblast), která:

a) poskytuje služby IT, nezbytné pro činnost úřadu k plnění úkolů vyplývající z působnosti úřadu,
b) je součástí úřadu a je nezbytné ji řídit, rozvíjet a provozovat v souladu s potřebami úřadu.

Pro strategické řízení ICT úřadu je nezbytné postupovat ve shodě s dokumentem „Celoměstská koncepce rozvoje informačních systémů pro potřeby hlavního města Prahy a městských částí na období 2013-2016“ a také s dokumentem „Schůzka členů Komise Rady HMP pro ICT s informatiky ÚMČ Prahy 1-22 a zástupci odboru informatiky MHMP“ konané dne 9. 2. 2015. Strategické směřování rozvoje ICT služeb je směrem k privátnímu cloudu a tím i technologiím, které jsou provozovatelné v prostředí cloudu. V současné době nejsou zřejmé následující informace:

- rozsah celopražských služeb
- technologická platforma
- časový harmonogram zavádění služeb
- financování a kofinancování
- nároky na síťovou propustnost a technologickou robustnost
- parametry poskytovaných služeb

V této etapě se dá očekávat, že spouštění těchto celopražských služeb probíhat postupně v delším časovém období v závislosti na finančních možnostech magistrátu viz Příloha č. 1.

5.1 AXIOMY ŘÍZENÍ INFORMATIKY IT

V souvislosti s řízením služeb IT i v souvislosti s případným využitím outsourcingu, je zapotřebí identifikovat axiomy řízení služeb IT úřadu. Tyto axiomy je potřebné vnímat v kontextu konkrétních podmínek úřadu. Jedná se zejména o následující:

1) Nepřenositelnost odpovědnosti

Za řízení IT služeb úřadu a zejména za ochranu dat nese ze zákona odpovědnost statutární zástupce. Ten může následně své povinnosti delegovat. Toto delegování pravomocí a odpovědností, aby bylo ve shodě s legislativou, musí být jednoznačné a prokazatelné. Správně definovaný a provozovaný outsourcing služeb IT lze považovat za jistou formou „prokazatelného delegování“ pravomocí za řešení těchto služeb, včetně odpovědnosti za jejich řešení.

2) Strategické řízení

Úřad může provozní záležitosti outsourcovat, ale strategické plánování a řízení by mělo vždy zůstat v jeho kompetenci. Pokud se vzdá strategického plánování a řízení, ztratí kontrolu i nad provozními záležitostmi bez ohledu na formu vlastního provozu, což je v přímém rozporu se všemi doporučeními a standardy pro řízení služeb.

3) Měřitelnost

Třetím axiomem je měřitelnost. Pokud úřad nenastaví jednoznačné a měřitelné parametry služeb a způsob jejich dokumentování a vyhodnocování, pak pravděpodobně nebude schopen vyhodnotit, zda služba funguje správně a zda jsou prováděné změny služeb k lepšímu, nebo horšímu. Pro nastavení těchto parametrů doporučujeme se držet známé metody SMART.

4) Vhodnost outsourcingu

Posledním axiomem je otázka vhodnosti outsourcingu pro jednotlivé služby. Pro posouzení vhodnosti outsourcingu platí, že **má-li poskytovatel služby plně odpovídat za funkčnost jím poskytované služby, musí mít odpovědnost za všechna aktiva, která jsou nezbytná k fungování této služby**.

Tento axiom ostatně platí pro provozování jakékoliv služby.

Vhodnost outsourcingu je ovlivňována vždy více faktory. K posouzení „vhodnosti“ outsourcingu je nezbytné identifikovat procesy související s řízením a provozem „Informatiky úřadu“ a z nich odvodit možnosti outsourcingu v daných oblastech. Na „vhodnost“ outsourcingu v dané oblasti mají vliv i další aspekty, zejména ekonomické a bezpečnostní.

5.2 SYSTÉM ŘÍZENÍ SLUŽEB IT

Informatiku úřadu lze definovat jako určitou entitu, poskytující služby v oblasti ICT. Poskytování těchto služeb je vhodné řídit v rámci zavedení určitého systému, např. systému managementu služeb IT dle normy ISO/IEC 20000.

Systém řízení služeb IT (SMS IT), implementovaný dle normy ISO/IEC 20000, představuje komplexní přístup pro řízení služeb poskytovaných informatikou úřadu, který je postaven na základě dlouhodobých a mezinárodně uznávaných pravidel a postupů pro řízení v oblasti IT.

Zavedením SMS pro řízení a provoz informatiky úřadu jsou definovány, nastaveny a dokumentovány procesy v oblasti řízení a provozu IT, což vytváří podmínky i pro účinné, efektivní a úspěšné využívání outsourcingu.

Jak je výše uvedeno, jedním ze způsobů řízení služeb IT je nastavení procesů v oblasti IT v souladu s normou ČNS ISO/IEC 20000-1, z roku 2012, která definuje požadavky na „Systém managementu služeb“ (SMS). V rámci SMS IT se službou rozumí jakékoliv prostředky, jimiž je zákazníkovi (externímu i internímu) dodávaná hodnota v podobě usnadnění výsledků, které chce zákazník dosáhnout.

Nastavení způsobů řízení informatiky, resp. služeb IT, na základě Systému managementu služeb dle ISO 20000 umožňuje jasné definice procesů, pravidel a postupů při řízení jednotlivých služeb IT, včetně jasného definování požadovaných parametrů služeb IT (co, v jaké kvalitě, termínech, s jakými zárukami, …). Tím jsou rovněž vytvářeny vhodné podmínky pro úspěšné nasazení outsourcingu v požadovaných oblastech.

Pro vytvoření představy o požadavcích normy ISO 20000 na systém řízení služeb IT je v následující kapitole uveden komentovaný souhrn těchto požadavků, procesů a jejich rozsah.

Současně je zde uvedeno hodnocení, jak přistoupit k jednotlivým oblastem požadavků normy ISO 20000 v podmínkách úřadu při řízení a při správě IT (tedy i ve vztahu k outsourcingu). Obecně pro každou oblast platí, že **strategické plánování a řízení je neoutsourcovatelné** a mělo by zůstat v kompetenci úřadu. Outsourcovat lze ve větší či menší míře provozní či realizační záležitosti každé z oblastí.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Hodnocení možnosti či nutnosti implementace procesů a požadavků normy ISO 20000 ve vztahu k outsourcingu je vyjádřeno následující formou, tj. symboly a barvami „semaforu“:

jednoznačně se doporučuje realizace procesu či požadavku na straně úřadu, definování a implementace má přímý vliv na řízení služeb v IT, resp. outsourcingu

realizace či implementace požadavku přímo neovlivňuje procesy související s outsourcingem, jejich realizace závisí na konkrétních podmínkách řízení IT při implementaci systému SMS

nedoporučuje se nebo není nutné realizovat při řízení IT v podmínkách úřadu MČ či využití outsourcingu

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

5.2.1 VŠEOBECNÉ POŽADAVKY NA SMS IT

Tato oblast řízení zahrnuje všeobecné požadavky na systém managementu služeb v IT. Ve své podstatě tyto požadavky vyplývají z obecných zásad řízení jakékoliv činnosti, a proto by tyto řídicí činnost měly být zavedeny a řízeny úřadem. Zavedení komplexního SMS IT není nezbytnou podmínkou, neboť implementace a zavedení SMS IT komplexně dle normy ISO 20000 má své výhody i nevýhody, vyžaduje nezbytné zdroje.

1. Všeobecné požadavky na systém managementu služeb IT	Doporučení k realizaci
1.1 Odpovědnost vedení úřadu za služby a jejich řízení Vedení úřadu má nezastupitelnou roli při plánování, zavedení, provozování, monitorování, udržování a zlepšování systému služeb IT, a to zejména stanovením rozsahu a cíli služeb, poskytováním zdrojů, přezkoumáváním SMS IT.	☺
1.2 Kontrola procesů provozovaných jinými stranami Všechny procesy provozovány jinými stranami (tj. např. outsourcing) musí být určeny, definovány a periodicky kontrolovány, a následně řízeny pomocí procesu řízení dodavatelů.	☺
1.3 Řízení dokumentace (dokumentů i záznamů) V rámci SMS jsou stanoveny požadované dokumenty a záznamy, které musí být vytvářeny a udržovány pro potřeby SMS IT. Musí být vytvořen systém řízení dokumentů a záznamů.	☺
1.4 Řízení zdrojů (poskytování zdrojů, lidské zdroje) Poskytovatel služeb musí určovat a poskytovat lidské, technické, informační a finanční zdroje potřebné pro zavedení a udržování SMS IT.	☺
1.5 Systém řízení služeb – ustanovení systému Poskytovatel služeb musí vymezit rozsah působnosti SMS IT a tento systém zavést. Po jeho zavedení musí poskytovatel služeb vytvořit a udržovat plán managementu služeb. Při plánování musí být zohledněna politika systému řízení služeb. .	😐
1.6 Systém řízení služeb - zlepšování systému Povinností poskytovatele služeb je provozovat SMS IT v souladu s plánem poskytování služeb a periodicky monitorovat a přezkoumávat tento systém. To představuje zavedení vhodných metody monitorování, např. interní audity a přezkoumání systému vedením.	😐

5.2.2 NÁVRH SLUŽEB A PŘECHOD NA NOVÉ NEBO ZMĚNĚNÉ SLUŽBY

Pro poskytování každé služby IT musí být použit proces pro návrh služeb, který zahrnuje níže uvedené požadavky. V podmínkách úřadu lze tyto požadavky vztáhnout i na IS, zajišťované v rámci služeb IT, případně na služby, které jsou poskytovány externím subjektem.

Zavedení nového informačního systému či služby IT, případně zavedení jejich změny, by měla být řízeno a spravováno dle níže uvedených požadavků normy ISO 20000. Ze strany úřadu je nutné pro tuto problematiku definovat pravidla a zavést je do praxe řízení IT, včetně outsourcingu.

2. Návrh služeb a přechod na nové nebo změněné služby	Doporučení k realizaci
2.1 Plánování nových nebo změněných služeb Pro každou novou službu, resp. změnu služby, musí být určeny požadavky na tuto službu. Nové nebo změněné požadavky musí být plánovány tak, aby naplnily požadavky na službu. Plánování nových nebo změněných služeb musí zahrnovat stanovené postupy.	☺
2.2 Návrh a vývoj nových nebo změněných služeb Návrh nové nebo změněné služby musí být dokumentován, musí zajistit naplnění určených požadavků na službu.	😐 *)
2.3 Přechod na nové nebo změněné služby Nové nebo změněné služby musí být testovány k ověření, zda naplňují požadavky na službu dle dokumentovaného návrhu služby. Pro nasazení musí být použit proces řízení uvolnění a nasazení.	☺

*) pouze v případě vývoje či návrhu nových služeb či informačních systémů.

5.2.3 PROCESY DODÁVKY SLUŽEB

Procesy dodávek služeb představují procesy související přímo s poskytováním konkrétních služeb a měly by být aplikovány při realizaci každé služby. Jejich aplikace je významná zejména při poskytování služby formou outsourcingu. Jedná se o procesy, které souvisejí s přímým řízením dodávek jednotlivých služeb, proto by minimálně vyznačené oblasti (viz ☺) měly být definovány a nastaveny na straně úřadu. Je zřejmé, že obdobně by měl outsourcer řídit své procesy dodávky služby, zejména tam, kde úřad řízení služby předává na stranu outsourcera, např. při řízení kapacit.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

3. Procesy dodávky služeb	Doporučení k realizaci
3.1 Management úrovně služeb Musí být nastaveny dohody o poskytovaných službách a jejich úrovni. Služby jsou definovány v katalogu služeb, s vyjádření vazeb mezi jednotlivými službami a stanoveny jednotlivé prvky služeb. Pro každou službu musí být sjednána dohoda o jejím poskytování s vyjádřením požadavků na její úroveň. Je potřebné provádět periodické přezkoumání služeb a dohod o jejich úrovních.	☺
3.2 Předkládání výkazů o službách Musí být stanoven a dokumentován popis každého výkazu o službě (službách). Výkazy o službách musí obsahovat údaje dle sjednané dohody o poskytování služby.	☺
3.3 Řízení kontinuity a dostupnosti služeb Musí být ohodnocena a dokumentována rizika související s kontinuitou a dostupnosti služeb. Požadavky na kontinuitu služeb musí být předem projednány a odsouhlaseny všemi zainteresovanými stranami. V požadavcích na kontinuitu je potřeba zohlednit požadavky na služby a dohody o úrovni služby. Musí být vytvořeny, zavedeny a udržovány plány kontinuity služby (služeb) a plány dostupnosti. Tyto plány musí být periodicky monitorovány a testovány.	☺
3.4 Rozpočtování a účtování služeb Musí existovat postupy a pravidla pro rozpočtování a účtování služeb (resp. jejich prvků). Rozpočtování musí umožnit efektivní finanční řízení služby. Náklady na poskytování služby musí být monitorovány a vykazovány ve vztahu k rozpočtu.	😐
3.5 Řízení kapacit Musí být odsouhlaseny a dokumentovány požadavky na kapacitu a výkonnost. Musí být zaveden a udržován plán kapacit (lidské, technické, informační a finanční zdroje). Využití kapacit musí být průběžně monitorováno a získané údaje o kapacitách musí být analyzovány.	😐
3.6 Řízení bezpečnosti informací Musí být schválena a zavedena bezpečnostní politika, poskytování služeb musí být v souladu s touto bezpečnostní politikou. Poskytovatel služby musí zavést fyzická, organizační, technická, administrativní a personální opatření k zajištění bezpečnosti v souladu s politikou bezpečnosti informací.	☺

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

5.2.4 PROCESY ŘÍZENÍ VZTAHŮ

Problematika řízení vztahů úzce souvisí s užíváním celého systému řízení služeb (pokud je zaveden). V podmínkách úřadu není nezbytné zavádět plně požadavky normy ISO 20000, ale je důležité se zaměřit zejména na ty oblasti, které souvisejí s poskytovanými službami, jako například problematika řízení a řešení stížností. Dále je to jednoznačné definování pravidel pro řízení dodavatelů, ty musí být ze strany úřadu definovány, nastaveny a kontrolovány.

4. Procesy řízení vztahů	Doporučení k realizaci
4.1 Řízení vztahů Musí být identifikováni zákazníci, uživatelé a zainteresované strany každé služby. Musí být nastavena pravidla komunikace. Musí existovat dokumentovaný postup pro řízení stížností na služby. Stížnosti musí být zaznamenány, prověřeny a řešeny.	😐
4.2 Řízení dodavatelů (pravidla pro řízení dodavatelů) Pro každého dodavatele musí být určena osoba odpovědná za řízení vztahu, smlouvy a výkonnost dodavatele. Vztah s dodavatelem musí být upraven smlouvou, stanovující mimo jiné dohodnutou úroveň služby, resp. služeb (SLA) Výkonnost dodavatelů musí být periodicky monitorována a měřena ve srovnání s cíli služeb. Změny ve smlouvě musí být řízeny pomocí procesu řízení změn.	☺

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

5.2.5 PROCESY ZAJIŠŤUJÍCÍ ŘEŠENÍ

Procesy se vztahují k záležitostem týkající se vzniku nestandardních situací, tzn. buď řízení incidentů a dále řízení problémů. Jednoznačně se jedná o procesy, které musí být definovány a nastaveny ze strany úřadu tak, aby v rámci outsourcingu byly využívány v případě potřeby. Jedná se významnou oblast, neboť vhodným nastavením lze předcházet eskalaci problémů do stavu s velkými dopady.

5. Procesy zajišťující řešení	Doporučení k realizaci
5.1 Řízení incidentů a žádostí o službu (pravidla pro identifikaci a záznam událostí) Pro řešení incidentů musí existovat dokumentovaný postup, zahrnující postupy od zaznamenání až po uzavření incidentu. Incidenty a žádosti o službu musí být řízeny v souladu s těmito postupy. Musí být odsouhlasena definice závažného incidentu. Závažné incidenty musí být řízeny dokumentovaným postupem, musí být přezkoumány s cílem nalezení příležitostí ke zlepšení.	☺
5.2 Řízení problémů (pravidla pro řešení událostí s dopadem na poskytované služby) Musí existovat postup pro identifikaci problémů a minimalizaci nebo předcházení dopadů incidentu a problémů. Problémy musí být řízeny v souladu s tímto postupem. Problémy vyžadující změny konfigurační položky služby musí být řešeny použitím žádosti o změnu.	☺

5.2.6 ŘÍDÍCÍ PROCESY

Jedná se o procesy související se řízením kvality služby, což je v podmínkách úřadu při využití outsourcingu velmi významné. Každá služba by měla být dokumentována pomocí tzv. „konfiguračních položek“, tzn. jednoznačné stanovení parametrů služby a jejich dokumentování v „konfigurační databázi“.

Tato definice a dokumentace služeb umožní řízení služeb, případně provedení jejich změny řízeným způsobem. Rovněž tak je velmi významná definice podmínek, za kterých může být nasazena nová služba, příp. jednotlivé součásti jejího provozního prostředí v případě jejich změny.

6. Řídicí procesy	Doporučení k realizaci
6.1 Řízení konfigurací (jednoznačná pravidla řízení konfigurací) Pro každou službu musí existovat definice služeb, a to definováním konfiguračních položek služby. Konfigurační položky musí být jednoznačně identifikovány a zaznamenány v konfigurační databázi (CMDB). Musí existovat pravidla pro řízení a správu CMDB.	☺
6.2 Řízení změn (jednoznačná pravidla pro řízení změn) Musí být stanovena politika pro řízení změn, určující, které konfigurační položky jsou tímto procesem řízeny. Rovněž tak musí být určena kritéria pro identifikaci změn se závažným dopadem na změny.	☺
6.3 Řízení uvolnění a nasazení Musí být ustanovena politika uvolnění nové či změněné služby. Služba před uvolněním musí být otestována. Uvolnění do provozního prostředí musí zachovat integritu HW, SW a dalších prvků služby.	☺

5.2.7 ZÁVĚR K SYSTÉMU ŘÍZENÍ SLUŽEB

Z výše uvedeného vyplývá, že požadavky normy ISO 20000 pokrývají celou šíři problematiky řízení IT prostřednictvím definováním služeb, poskytovaných IT. Ve vztahu k problematice outsourcingu části nebo všech služeb informatiky úřadu vyplývá, že definování a nastavení parametrů většiny služeb musí být **provedeno na straně úřadu.**

Tento požadavek nezakládá povinnost, či potřebu zavést komplexně systém řízení služeb IT dle normy ISO 20000, ale je **potřebné definovat a zavést procesy pro řízení služeb a dále definovat parametry služeb úřadem před jejich případným outsourcováním.**

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

6 BALÍČKY SLUŽEB

Jedním ze základních prvků řízení jakosti služeb je problematika Managementu konfigurací.

Obsahem Managementu konfigurací je stanovení a sledování konfigurací jednotlivých aktiv úřadu. Pro potřeby zpracování požadovaných variant se zde budeme zabývat převážně hardwarovým a softwarovým vybavením. Znalost přesného nastavení těchto aktiv je velmi důležitá hlavně pro poskytování uživatelské podpory, provádění nových implementací nebo auditů.

Management konfigurací můžeme definovat takto:

Management konfigurací je proces standardizace zdrojů konfigurace a prosazování jejich stavu v celé IT infrastruktuře. Management konfigurací je rozhodující pro úspěch jiných IT procesů, včetně poskytování služeb, řízení změn, Release Management, Patch Management, dodržování předpisů a bezpečnosti.

Tento management definuje všechny požadavky a měřitelné parametry pro dané aktivum. Následující výčet oblastí je výčtem obvyklých problematik definovaných v managementu konfigurací:

- Požadavky na dostupnost a provoz (zejména časy)
- Personální požadavky
- HW a SW požadavky
- Požadavky na SLA
- Popis rozhraní/ API
- Popis integračních vazeb
- Popis požadované konektivity
- Požadavky na zálohování a D&R
- Požadavky na ochranu informací

Postupy, procesy a pravidla pro stanovení a kontrolu služeb dle managementu konfigurací zajišťuje systém řízení jakosti služeb a systém řízení bezpečnosti informací. Požadavky na jednotlivá aktiva v managementu konfigurací jsou základním východiskem pro specifikaci RfP.

Dle požadavku ZD jsou dále navrženy „balíčky“, tj. skupiny služeb/aktiv/požadavků. Každý tento balíček by na základě principu plné zodpovědnosti za fungování služby měl být dále nedělitelný. Pokud by došlo k dalšímu rozdělení, pak výrazně vzrostou požadavky na koordinaci a řízení na straně úřadu, zvýší se rizika spojená s dostupností služby a zvýší se personální a tím i finanční nároky na straně úřadu. Zejména finanční nároky v oblasti personální mohou vést k neřešitelnému problému – nenalezení pracovníka s požadovanou kvalifikací v rámci úřadem definovaného finančního rámce.

S ohledem na postupné zprovozňování služeb magistrátem, ukazuje se jako výhodné, zahrnout další parametr balíčku – délku poskytování. Během doby poskytování služby, může dojít k tomu, že služba bude nabídnuta jiným subjektem (magistrátem či MČ) a pro objednatele bude výhodnější přejít na službu novou.

Z toho vyplývá, že i když budou jednotlivé baličky vybírány na předem stanovené období, již při nákupu by měly být definovány podmínky jejího předčasného ukončení. Tyto podmínky by měly být jedním z kritérií při výběru poskytovatele.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Definice balíčků:

A. Aktiva specifikovaná v části D1 projektu. Tato aktiva jsou reprezentována HW + OS + SW. Problematiku LAN a WAN je možno vydělit jako samostatné balíčky s tím, že požadavky a parametry musí reflektovat požadavky hlavních aktiv. Je zřejmé, že pro funkčnost příslušné služby (hlavního aktiva) je bezpodmínečně nutné zajistit funkčnost všech podpůrných aktiv, na kterých je hlavní aktivum závislé. Úřad pro potřeby RfP specifikuje požadovanou minimální konfiguraci podpůrných aktiv s výhledem vyhovující morální úrovně po dobu 5 let. Tento **neobsahuje** koncové stanice (PC a NB).

B. Tento **balíček je tvořen** koncovými stanicemi (PC a NB). Zde je nezbytné nastavit systém řízení jakosti služeb tak, aby byly dodrženy požadavky na fix time a další parametry aktiv, které stanoví úřad.

C. LAN – podpůrné aktivum sdílené hlavními aktivy. Úřad definuje minimální propustnost LAN sítě/segmentů sítě, redundanci, bezpečnostní a provozní parametry sítě a případně cíle rozvoje, kterých má být během outsourcingu dosaženo (např. HA).

D. WAN – podpůrné aktivum sdílené některými hlavními aktivy, obvykle již rovnou nakupovaná služba. Úřad definuje minimální propustnost WAN, redundanci, bezpečnostní a provozní parametry sítě a případně cíle rozvoje, kterých má být během outsourcingu dosaženo.

E. Řízení bezpečnosti informací (ISMS) – možno outsourcovat z pohledu realizace opatření, nikoli z pohledu strategického řízení.

F. Bezpečnost informací – bezpečnostní prvky – outsourcing společně s příslušnými balíčky. Úřad musí stanovit cíle bezpečnosti, aby poskytovatel služby věděl, čeho má bezpečnostními prvky dosáhnout. Tato problematika je obvykle/zvykově dělena na:
   - Zpracování logů (HW, SW, LAN prvky) pomocí SIEM systémů
   - Firewally, IDS, IPS pro WAN, někdy i LAN (oddělená vnitřní síť od serverů)
   - Shoda s legislativou, požadavky na záznamy

G. Tisky – outsourcing jak tiskáren, tak spotřebního materiálu a řízení tisku (přehled o objemech, řízení práv tisku atd.). Úřad musí stanovit požadavky na tiskárny, jaké služby k nim požaduje, případně bezpečnostní omezení pro stanovená pracoviště. Tento balíček definuje kompletní požadavky na tisk a před vlastní soutěží je třeba zvážit ukončení stávajících smluv a provedení optimalizace tisků.
   Na základě zjištěných informací se touto problematikou zabývá odlišný segment dodavatelů než v oblasti SW a HW. Z tohoto důvodu doporučujeme tento balíček soutěžit samostatně. Toto není podmínkou, ale pouze doporučení.

H. Call centrum – outsourcing služby pro občany. Úřad musí stanovit parametry služby. Jedním z parametrů by měla být doba poskytování služby (např. 5x10), dalším může být i délka čekání volajícího na lince.

I. Help Desk – systém pro zaměstnance úřadu pro hlášení požadavků, chyb, problémů … Tento systém by měl sloužit pro celý úřad a pro všechny oblasti a distribuovat požadavky na jednotlivé partnery. Nároky na Help Desk stoupají s počtem „autonomních systémů“.

J. Web – veřejný web P10 – je vhodné outsourcovat jeho provoz, nikoli redakční činnost.

K. Telefony (mobil, ústředna) – problematika mobilních telefonů a pevných linek je již dnes, z principu, outsourcingem (nákup externí služby). Zde tedy jde pouze o stanovení požadavků a výběr vhodného poskytovatele. Interní linky obsluhované interní ústřednou je možno také outsourcovat včetně koncových zařízení. Pokud úřad přistoupí k tomuto kroku, je vhodné toto řešit tak, aby bylo možno realizovat konfigurace služeb ve shodě s požadavky mobilů a pevných linek. Dalším otazníkem je přechod na IP telefonii.

Dále uváděné varianty jsou sestaveny ze zde definovaných balíčků. Jednotlivé varianty jsou navrženy tak, aby bylo možno zvolit optimální rozsah služby, případně i obdobný jako je současný outsourcing, bez tiskových služeb, poskytovaný O2.

Jednotlivé varianty outsourcingu byly navrženy s ohledem na legislativní prostředí ČR, zkušenosti zpracovatele a požadavky vedoucích pracovníků úřadu.

Při sestavení variant byly zohledněny zejména:

Zákon č. 101/2000 Sb., o ochraně osobních údajů

§ 6

Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.

Zákon č. 137/2006 Sb., o veřejných zakázkách

§ 13

Předpokládaná hodnota veřejné zakázky

(1) Předpokládanou hodnotou veřejné zakázky se pro účely tohoto zákona rozumí zadavatelem předpokládaná výše peněžitého závazku vyplývající z plnění veřejné zakázky, který je zadavatel povinen stanovit pro účely postupu v zadávacím řízení před jeho zahájením. Při stanovení předpokládané hodnoty je vždy rozhodná cena bez daně z přidané hodnoty.

(2) Předpokládanou hodnotu stanoví zadavatel v souladu s pravidly stanovenými v tomto zákoně a na základě údajů a informací o zakázkách stejného či podobného předmětu plnění; nemá-li zadavatel k dispozici takové údaje, stanoví předpokládanou hodnotu na základě údajů a informací získaných průzkumem trhu s požadovaným plněním, popřípadě na základě údajů a informací získaných jiným vhodným způsobem. Pro stanovení výše předpokládané hodnoty je rozhodný den odeslání oznámení či výzvy o zahájení zadávacího řízení k uveřejnění.

(3) Zadavatel nesmí rozdělit předmět veřejné zakázky tak, aby tím došlo ke snížení předpokládané hodnoty pod finanční limity stanovené v tomto zákoně.

(4) **Je-li veřejná zakázka rozdělena na části, je pro stanovení předpokládané hodnoty rozhodující součet předpokládaných hodnot všech částí veřejné zakázky.**

(5) V případě, že zadavatel poskytuje účastníkům soutěže o návrh či účastníkům soutěžního dialogu odměny, soutěžní ceny či jiné platby, zahrnuje předpokládaná hodnota i výši těchto odměn, soutěžních cen či jiných plateb.

(6) Pokud si zadavatel v zadávacích podmínkách vyhradil opční právo podle § 99, musí předpokládaná hodnota zahrnovat rovněž předpokládanou hodnotu všech veřejných zakázek na dodávky, služby či stavební práce požadovaných zadavatelem při využití opčního práva; zadavatel je v takovém případě současně povinen zvlášť stanovit předpokládanou hodnotu veřejné zakázky na dodávky, služby či stavební práce a předpokládanou hodnotu dodávek, služeb nebo stavebních prací při využití opčního práva.

(7) V případě rámcových smluv a dynamického nákupního systému je předpokládanou hodnotou maximální předpokládaná hodnota všech veřejných zakázek, které mají být zadány za dobu trvání rámcové smlouvy či dynamického nákupního systému.

(8) Při stanovení předpokládané hodnoty je zadavatel povinen sečíst předpokládané hodnoty obdobných, spolu souvisejících dodávek či služeb, které hodlá pořídit v průběhu účetního období. To neplatí pro dodávky nebo služby, jejichž jednotková cena je v průběhu účetního období proměnlivá a zadavatel tyto dodávky nebo služby pořizuje opakovaně podle svých aktuálních potřeb; zadavatel je však povinen vždy dodržet zásady podle § 6 odst. 1.

§ 98

Zadávání částí veřejných zakázek

(1) Zadavatel může rozdělit veřejnou zakázku na části, připouští-li to povaha předmětu veřejné zakázky.

(2) V případě rozdělení veřejné zakázky na části uvede zadavatel tuto skutečnost v oznámení či výzvě o zahájení zadávacího řízení a vymezí předmět jednotlivých částí veřejné zakázky a další požadavky související s rozdělením veřejné zakázky na části.

(3) Pokud zadavatel rozdělil veřejnou zakázku na části, uvede v oznámení či výzvě o zahájení zadávacího řízení, zda je dodavatel oprávněn podat nabídku na všechny či některé části veřejné zakázky nebo jen na jednu část veřejné zakázky.

(4) Je-li veřejná zakázka rozdělena na části, vztahují se ustanovení tohoto zákona týkající se postupů zadavatele v zadávacím řízení či práv a povinností dodavatele na každou jednotlivou část, nevyplývá-li z tohoto zákona jinak. Ustanovení § 13 odst. 4 tím není dotčeno.

(5) Vyplývá-li z povahy plnění, že je možné předmět nadlimitní veřejné zakázky na dodávky, služby či stavební práce rozdělit na jednotlivé části, je zadavatel oprávněn zadat tyto části dodávek, služeb či stavebních prací postupem stanoveným pro podlimitní veřejné zakázky za předpokladu, že předpokládaná hodnota příslušné části v případě dodávek a služeb je nižší než částka odpovídající 80 000 EUR a v případě stavebních prací nižší než částka odpovídající 1 000 000 EUR, a dále za předpokladu, že celková předpokládaná hodnota všech takto zadávaných částí nepřesáhne 20 % předpokládané hodnoty předmětu celé veřejné zakázky. Ustanovení § 19 odst. 1 tím není dotčeno.

Dále při návrhu jednotlivých variant bylo přihlédnuto ke zkušenostem vedoucích pracovníků úřadu s aktuálním stavem v problematice tiskových služeb. Zde dochází k naplnění rizika při dvou zodpovědných osobách, tj. dílčí služba, dle poskytovatele, je funkční, ale obě služby jako celek vykazují vady. Úřad není schopen doložit kdo je viníkem daného stavu, tudíž není schopen ani účinně použít sankční ujednání.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Tento zákon se sice dnes nevztahuje na informační systémy, jejichž správcem je obec či městská část při výkonu působnosti obce (zákon č. 128/2000 Sb.), je však vhodným etalonem pro stanovení míry kybernetické a informační bezpečnosti, navíc lze očekávat, že působnost zákona o kybernetické bezpečnosti bude na obce v dohledné době rozšířena.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Důležitým faktorem je souhrn požadavků na maximální délku výpadku jednotlivých aktiv (systémů).

Aktivum	Max. doba výpadku
Czech Point	1h
Agendio	1h
Data Centrum	1d (v rámci jednoho pracovního dne)
DES/iDES	4h (v rámci jednoho pracovního dne)
e-spis	1h
GINIS	3h (v rámci jednoho pracovního dne)
Intranet	4h (v rámci jednoho pracovního dne)
ICZ - RZP - živnostenská agenda	1h
OK nouze	1d (v rámci jednoho pracovního dne)
VITA - Stavební úřad	1h
5M.DAT	1d (v rámci jednoho pracovního dne)
ASPI	1d
Avast	1d
Call Centrum	1d
CC Navigátor	1d
Doprava	2d
El. podatelna firmy AEC	1h
ELO enterpice/client	1d
EVI	2d
Generel zeleně	3d
InfoMapa	3d
InPakom	1d
MISYS/webMISYS	1d
Persnet	1d
SDEKO	1d
SEM	1d
VITA - Přestupky	1h
Audit Pro	dle potřeby - není používáno stále
Benefit	4h (v rámci jednoho pracovního dne)
Firemní právník	2d
Internet - ESO	2d
Q-MATIC	1h
Help desk	1d
Symantec Antivirus	1h
MS Office 2013	na lokálních stanicích – fix time dle místa použití
Zoner photo studio	na lokálních stanicích – 2d
Kadlec elektro - vyvolávací systém	1h
ONYF	2d
MS Exchange server	1h
SharePoint Learning	2d

Kde jsou:

- h – hodina
- d - den

Tabulka vznikla na základě interview s odpovědnými pracovníky úřadu, časy v ní uváděné jsou maximální akceptovatelné časy výpadku dle respondentů.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Při rozdělení variant 1 nebo 2 na více výběrových soutěží je vhodné zůstat ve shodě s výše uvedenými texty, zákony a požadavky úřadu. Jednou zcest by mohla být realizace všech dílčích soutěží ve stejném režimu jako největší soutěž. Tento postup by mohl být velice náročný jak na organizaci, tak na čas a bez garance včasného úspěšného dokončení všech soutěží. Zde při takovémto rozdělení je nezbytné dostatečné personální zajištění na straně úřadu pro organizaci soutěží, zabezpečení požadavků úřadu nebo pro řízení jednotlivých SLA a dodržení požadovaných fix time. Tím však může být snížena případná možná finanční výhodnost takovéhoto kroku. Požadavky na rozdělení doporučených variant z důvodu „že bude dosaženo výhodnější ceny“ nejsou zcela prokazatelné. V případě realizace více SLA nebo kombinaci interního a externího zajištění je nutno předpokládat následující **další náklady** z důvodu řízení a minimalizace rizik:

- Vzroste cena za monitorovací nástroje a Help Desk (náročnější a detailnější monitorování stavu)
- Vzroste počet pracovníků, kteří se musí zabývat řízením služeb
- Vzroste náročnost na dodržení dostupnosti celkové služby (dílčí služby mohou být v pořádku, ale celková služba nemusí být plně funkční)
- Vznikne potřeba role architekta systému, tj. další pracovní místo
- Vznikne potřeba role bezpečnostního ředitele, tj. řízení bezpečnosti napříč jednotlivými dílčími službami

V části 3 projektu budou navržena jednotlivá RfP. Tato RfP budou připravena na základě rozhodnutí úřadu a v takové skladbě, jakou toto rozhodnutí určí[1].

[1] Ve shodě s platnou smlouvou

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

7 VARIANTA 1

Tato varianta předpokládá zajištění jednou smlouvou, tj. za zajištění služeb, jejich jakost a dodržení parametrů je zodpovědný **právě jeden smluvní partner**. Důvodem je nejvyšší míra minimalizace rizik spojených s provozem a řízením veškerých služeb. Tímto smluvním partnerem může být i partner se subdodavateli či konsorcium dodavatelů s jasnou garancí funkčnosti a zodpovědností. Tento postup je adekvátní alternativou pro vznesené požadavky na rozdělení soutěže do více zakázek, kde důvodem je možnost účasti i menších nebo specializovaných subjektů.

Tímto postupem také nedochází k možnému umělému dělení veřejné zakázky.

Časový rozsah je předpokládán:

- V úřední dny od 8:00 do 19:00
- V neúřední dny od 8:00 do 16:00

Tato varianta je tvořena následujícími balíčky:

A. Aktiva specifikovaná v části D1 projektu. Tato aktiva jsou reprezentována HW + OS + SW. Problematiku LAN a WAN je možno vydělit jako samostatné balíčky s tím, že požadavky a parametry musí reflektovat požadavky hlavních aktiv. Je zřejmé, že pro funkčnost příslušné služby (hlavního aktiva) je bezpodmínečně nutné zajistit funkčnost všech podpůrných aktiv, na kterých je hlavní aktivum závislé. Úřad pro potřeby RfP specifikuje požadovanou minimální konfiguraci podpůrných aktiv s výhledem vyhovující morální úrovně po dobu 5 let. Tento neobsahuje koncové stanice (PC a NB).

B. Tento balíček je tvořen koncovými stanicemi (PC a NB). Zde je nezbytné nastavit systém řízení jakosti služeb tak, aby byly dodrženy požadavky na fix time a další parametry aktiv, které stanoví úřad.

C. LAN – podpůrné aktivum sdílené hlavními aktivy. Úřad definuje minimální propustnost LAN sítě/segmentů sítě, redundanci, bezpečnostní a provozní parametry sítě a případně cíle rozvoje, kterých má být během outsourcingu dosaženo (např. HA).

E. Řízení bezpečnosti informací (ISMS) – možno outsourcovat z pohledu realizace opatření, nikoli z pohledu strategického řízení.

F. Bezpečnost informací – bezpečnostní prvky – outsourcing společně s příslušnými balíčky. Úřad musí stanovit cíle bezpečnosti, aby poskytovatel služby věděl, čeho má bezpečnostními prvky dosáhnout. Tato problematika je obvykle/zvykově dělena na:

- Zpracování logů (HW, SW, LAN prvky) pomocí SIEM systémů
- Firewally, IDS, IPS pro WAN, někdy i LAN (oddělená vnitřní síť od serverů)
- Shoda s legislativou, požadavky na záznamy

I. Help Desk – systém pro zaměstnance úřadu pro hlášení požadavků, chyb, problémů … Tento systém by měl sloužit pro celý úřad a pro všechny oblasti a distribuovat požadavky na jednotlivé partnery

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

8 VARIANTA 2

Tato varianta nepředpokládá zajištění služeb jednou smlouvou. Služby s menšími nároky na kvalitu, dobu bez výpadku atd. lze zajistit interními zdroji nebo případně soutěžit samostatně bez vazby (ve smyslu zákona o veřejných zakázkách) na hlavní soutěž/smlouvu. Takovými službami může být provoz LAN, pořízení a podpora pracovních stanic apod.

Tímto postupem by nemělo dojít k možnému umělému dělení veřejné zakázky, protože to jsou služby víceméně autonomní s hlavní službou minimálně související

Časový rozsah je předpokládán:

- V úřední dny od 8:00 do 19:00
- V neúřední dny od 8:00 do 16:00

Tato varianta je tvořena následujícími balíčky v outsourcingu:

A. Aktiva specifikovaná v části D1 projektu. Tato aktiva jsou reprezentována HW + OS + SW. Problematiku LAN a WAN je možno vydělit jako samostatné balíčky s tím, že požadavky a parametry musí reflektovat požadavky hlavních aktiv. Je zřejmé, že pro funkčnost příslušné služby (hlavního aktiva) je bezpodmínečně nutné zajistit funkčnost všech podpůrných aktiv, na kterých je hlavní aktivum závislé. Úřad pro potřeby RfP specifikuje požadovanou minimální konfiguraci podpůrných aktiv s výhledem vyhovující morální úrovně po dobu 5 let. Tento neobsahuje koncové stanice (PC a NB).

B. Tento balíček je tvořen koncovými stanicemi (PC a NB). Zde je nezbytné nastavit systém řízení jakosti služeb tak, aby byly dodrženy požadavky na fix time a další parametry aktiv, které stanoví úřad.

F. Bezpečnost informací – bezpečnostní prvky – outsourcing společně s příslušnými balíčky. Úřad musí stanovit cíle bezpečnosti, aby poskytovatel služby věděl, čeho má bezpečnostními prvky dosáhnout. Tato problematika je obvykle/zvykově dělena na:

- Zpracování logů (HW, SW, LAN prvky) pomocí SIEM systémů
- Firewally, IDS, IPS pro WAN, někdy i LAN (oddělená vnitřní síť od serverů)
- Shoda s legislativou, požadavky na záznamy

I. Help Desk – systém pro zaměstnance úřadu pro hlášení požadavků, chyb, problémů … Tento systém by měl sloužit pro celý úřad a pro všechny oblasti a distribuovat požadavky na jednotlivé partnery

Tato varianta je dále tvořena následujícími balíčky realizovanými úřadem:

C. LAN – podpůrné aktivum sdílené hlavními aktivy. Úřad definuje minimální propustnost LAN sítě/segmentů sítě, redundanci, bezpečnostní a provozní parametry sítě a případně cíle rozvoje, kterých má být během outsourcingu dosaženo (např. HA).

E. Řízení bezpečnosti informací (ISMS) – možno outsourcovat z pohledu realizace opatření, nikoli z pohledu strategického řízení.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Balíčky B, F, I je možno (na základě rozhodnutí úřadu) řešit formou outsourcingu nebo interními zdroji. Ze je třeba klást důraz na řešení rizik a postupů provázaností těchto služeb, zejména s ohledem na integraci a parametry služeb (aktiv).

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

9 VARIANTA 3

Tato varianta obsahuje všechny balíčky dle Varianty 1 z důvodu požadovaného cenového srovnání mezi variantami, i když je realizována interními zdroji. Pro ocenění této varianty jsou požity ceny z veřejně dostupných koncových ceníků výrobců/poskytovatelů údajů a kvalifikovaného odhadu.

Časový rozsah je předpokládán:

- V úřední dny od 8:00 do 19:00
- V neúřední dny od 8:00 do 16:00

Tato varianta je tvořena následujícími balíčky:

A. Aktiva specifikovaná v části D1 projektu. Tato aktiva jsou reprezentována HW + OS + SW. Problematiku LAN a WAN je možno vydělit jako samostatné balíčky s tím, že požadavky a parametry musí reflektovat požadavky hlavních aktiv. Je zřejmé, že pro funkčnost příslušné služby (hlavního aktiva) je bezpodmínečně nutné zajistit funkčnost všech podpůrných aktiv, na kterých je hlavní aktivum závislé. Úřad pro potřeby RfP specifikuje požadovanou minimální konfiguraci podpůrných aktiv s výhledem vyhovující morální úrovně po dobu 5 let. Tento neobsahuje koncové stanice (PC a NB).

B. Tento balíček je tvořen koncovými stanicemi (PC a NB). Zde je nezbytné nastavit systém řízení jakosti služeb tak, aby byly dodrženy požadavky na fix time a další parametry aktiv, které stanoví úřad.

C. LAN – podpůrné aktivum sdílené hlavními aktivy. Úřad definuje minimální propustnost LAN sítě/segmentů sítě, redundanci, bezpečnostní a provozní parametry sítě a případně cíle rozvoje, kterých má být během outsourcingu dosaženo (např. HA).

E. Řízení bezpečnosti informací (ISMS)

F. Bezpečnost informací – bezpečnostní prvky. Úřad musí stanovit cíle bezpečnosti, aby poskytovatel služby věděl, čeho má bezpečnostními prvky dosáhnout. Tato problematika je obvykle/zvykově dělena na:

- Zpracování logů (HW, SW, LAN prvky) pomocí SIEM systémů
- Firewally, IDS, IPS pro WAN, někdy i LAN (oddělená vnitřní síť od serverů)
- Shoda s legislativou, požadavky na záznamy

I. Help Desk – systém pro zaměstnance úřadu pro hlášení požadavků, chyb, problémů … Tento systém by měl sloužit pro celý úřad a pro všechny oblasti a distribuovat požadavky na jednotlivé partnery.

Z hlediska časového i s ohledem na zajištění bezpečnosti se tato varianta jeví, v plném rozsahu, jako obtížně realizovatelná.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

10 SROVNÁVACÍ ANALÝZA

V této části se budeme zabývat finanční hodnotou jednotlivých částí pro potřeby interního provozování a porovnáním výhod a nevýhod variant outsourcingových a interního provozování.

10.1 POROVNÁNÍ VYBRANÝCH PARAMETRŮ STÁVAJÍCÍCH SMLUV

V následující tabulce jsou uvedeny vybrané informace ze současných smluv poskytnutých úřadem.

název projektu	trvání & vypovězení	prac. doba
Dodávky cartridgí a tonerů pro tiskárny ÚMČ Praha 10	smlouva na neurčito, výpovědní doba 3 měsíce	dle objednávky nebo potřeby
Údržba a služby pro zabezpečení provozu dodaného díla "Interaktivní úřední deska" (HW i SW)	smlouva na 2 roky, prodloužení o rok, pokud není řečeno jinak	dle objednávky nebo potřeby
Smlouva o pronájmu diskového prostoru a poskytování souvisejících služeb	neurčito, výpovědní lhůta 3 měsíce a předplatné propadá	dle objednávky
Smlouva o poskytování služeb elektronických komunikací - internet	neurčito, výpovědní lhůta 3 měsíce	
Smlouva o poskytování odborného servisu	neurčito, výpovědní lhůta 3měsíce, vyrovnáni do 30 dnů od ukončení smlouvy	k disposici od 7:00-17:00,18:00-22:00
Smlouva o poskytování elektronických komunikací - server housing	neurčito, výpovědní lhůta jsou 3měsíce	
Smlouva o technickém zajištění obsluhy systémů	výpověď možná bez udání důvodu, výpovědní lhůta jsou 3 měsíce, výpověď možná po 6 měsících plnění,	
Smlouva o poskytování služby Webcall	na neurčito, 2 měsíce výpovědní lhůty - bez udání důvodu	
Mobílní služby	Do 03/2016, možnost prolongace	
Smlouva o nájmu multifunkčních zařízení a souvisejících služeb	60 měsíců, výpovědní lhůta jsou 3 měsíce i bez udání důvodu	
Smlouva zajištění běžného provozu a rozvoje portálů a dalších webových presentací MČ Praha 10	36 měsíců, výpovědní lhůta 3 měsíce - i bez udání důvodu,	evidence chyb oprav a hodin 7x24
Smlouva o poskytování služeb provozu webových presentací Prahy 10 - servisní smlouva	24 měsíců, výpovědní lhůta jsou 3 měsíce,	evidence chyb oprav a hodin 7x24, údržba 5x8, správa serveru 24x7, poskytovatel přijímá hlášení poruch 5x8

Z uvedeného přehledu vyplývá, že parametry služeb jsou různorodé a v různé šíři. Není zřejmá vazba mezi parametry smlouvy a požadavky na kvalitu služby definovanou úřadem. Doporučujeme zavést řízení jakosti služeb pro ICT a tím umožnit lepší specifikaci potřeb úřadu.

10.2 PERSONÁLNÍ POROVNÁNÍ

Pro zabezpečení služeb a kontinuity služeb ICT je nezbytné disponovat kvalifikovaným personálem. Tento personál může být v zaměstnaneckém vztahu k úřadu nebo tento personál zajišťuje poskytovatel outsourcingu.

Zde není řešena problematika personálu na straně úřadu, který je nezbytný pro všechny tři varianty – tzv. koordinátor. Tuto roli musí zajistit úřad při všech variantách. Pro tuto roli je nezbytné také řešit zastupitelnost.

V případě Varianty 3 musí úřad počítat se zajištěním pracovních míst pro jednotlivé pracovníky (kanceláře a jejich vybavení).

V následující tabulce je uvedeno kdo zajišťuje definované oblasti v případě outsourcingu. Pokud by nebyl outsourcing, pak všechny tyto oblasti musí zajistit úřad.

Oblast	**Poskytovatel outsourcingu**	**Úřad**
Nezbytné kvalifikace	Parametry outsourcingu	Požadavky
Zastupitelnost	Poskytovatel outsourcingu	-
Vzdělávání	Poskytovatel outsourcingu	-
Personální agenda	Poskytovatel outsourcingu	-
Agenda řízení	Poskytovatel outsourcingu	-

Následující tabulka definuje základní okruhy problematik z pohledu personalistiky úřadu v rozdělení interního zajištění a outsourcingu.

Personální zabezpečení z pohledu úřadu	
Interní pracovník	**Outsourcing**
Mzda	Pouze měsíční paušál
Školení	
Odborná zdatnost	
Administrativa a řízení	
Personalistika	
Nemoci	
Dovolené	
Využití pracovní doby	
Zabezpečení personálu	

V současné situaci by musel úřad znovu vybudovat celé oddělení informatiky. Zde je třeba zdůraznit problematiku náboru pracovníků s požadovanou kvalifikací. Tento nábor si vyžádá určitý, těžko specifikovatelný, čas.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

10.3 TECHONOLOGICKÉ POROVNÁNÍ

Pro zabezpečení kvality a kontinuity služeb ICT je nezbytné reflektovat požadavky úřadu a požadavky provozovaných IS/SW. Tyto technické požadavky, zejména jejich změny, je třeba řešit v čase.

Následující tabulka definuje rozdíl mezi outsourcingem a interním provozem (oblast HW) pro dané oblasti.

Oblast	Outsourcing	Interní provoz
Morální úroveň HW	Skoková obnova	Postupná obnova (většinou řešení havarijního stavu)[2]
Obnova HW	Skoková a dle parametrů SLA	Postupná obnova (většinou řešení havarijního stavu)[3]
Servis a jeho řízení	Přenesení řízení partnerů na poskytovatele služby	Mnoho partnerů, řízení vztahu mezi nimi
Technická podpora a její řízení	Přenesení řízení dodavatelů na poskytovatele služby	Mnoho dodavatelů, řízení vztahu mezi nimi

Následující tabulka definuje rozdíl mezi outsourcingem a interním provozem (oblast SW a OS) pro dané oblasti.

Oblast	Outsourcing	Interní provoz
Licence SW	Služba správy licencí	Potřeba specialisty
Řízení licencí SW	Služba řízení licencí (kvalita provozu)	Potřeba specialisty
Správa provozu IS/SW	Přenesení řízení partnerů na poskytovatele služby	Mnoho partnerů, řízení vztahu mezi nimi
Technická podpora a její řízení	Přenesení řízení partnerů na poskytovatele služby	Mnoho partnerů, řízení vztahu mezi nimi
Integrace IS	Přenesení řízení partnerů na poskytovatele služby	Mnoho partnerů, řízení vztahu mezi nimi

Stav technologií a potřeby úřadu (zejména obnova centrálních serverů a koncových stanic) v současné době hovoří spíše pro realizaci outsourcingu. Interní provoz předpokládá nábor zaměstnanců, zavedení celého, ne jenom strategické části, systému řízení jakosti služeb a nastavení vztahů s dodavateli.

10.4 JAKOST SLUŽEB

Pro zabezpečení kvality služeb je nezbytné nastavit očekávanou kvalitu (definovat co je to kvalita – jak bude měřena).

Následující tabulka popisuje situaci za předpokladu outsourcingu.

Oblast	Poskytovatel outsourcingu	Úřad
Stanovení kvality	Nastavuje zabezpečení	Definuje
Naplnění kvality	Realizuje	Kontroluje
Personál	Zabezpečuje a řídí	-
Technika	Zabezpečuje	Stanovuje strategii
SW	Zabezpečuje	Stanovuje strategii
Integrační vazby	Zabezpečuje	Stanovuje strategii

V případě interního řešení musí vše zajistit úřad. V případě outsourcingu je toto pro úřad jednodušší.

[2] Zvýšené riziko nedodržení fix time z důvodu nefunkčnosti zařízení
[3] Zvýšené riziko nedodržení fix time z důvodu nefunkčnosti zařízení

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

10.5 POROVNÁNÍ ICT

Tabulka porovnává problematiku řízení informatiky (OIN) bez a s outsourcingem.

Parametr	Bez zavedení outsourcingu	S pokračováním outsourcingu
Služby občanům (portál občana, řešení životních situací atd.)	(-) Vazba na rozvoj ICT a proto dlouhodobý rozvoj v období 2015-2020	(+) Nabídka nových služeb občanům
Rychlost modernizace ICT	(-) Postupná obnova	(+) Rychlá, jednorázová modernizace je možná již během prvního roku outsourcingu
Počet pracovníků úřadu v oblasti ICT	(-) Zvýšení počtu pracovníků OIN	(+) Zachování počtu pracovníků OIN
Plánování výdajů na ICT ve střednědobém horizontu	(-) Obtížně plánovatelné	(+) Fixně plánované
Úroveň a kvalita služeb	(-) Stagnující, případně postupné zvyšování	(+)Trvalý zájem dodavatele o kvalitní služby (v opačném případě přichází o peníze)
Bezpečnost	(-) Stagnující, případně postupné zvyšování	(+)Trvalý zájem dodavatele o řešení bezpečnosti (v opačném případě přichází o peníze)
Náklady na ICT	(-) Konstantní pro udržení provozu, při výdajích do potřebných investic jejich navýšení	(+) Fixní částka pro období platnosti kontraktu s externí firmou
Náročnost změny (smluvní ujednání a jejich změny)	(+) Nízká náročnost změny	(-) Vysoká náročnost změny

Toto porovnání ukazuje, že akceschopnost úřadu v problematice ICT, je ovlivněna:

- Nastaveným způsobem řízení
- Úrovní rozhodovacích pravomocí
- Strategií úřadu v této oblasti

10.6 SYSTÉM ŘÍZENÍ – POROVNÁNÍ

Pro zabezpečení kvality a kontinuity služeb ICT je nezbytné nastavit pravidla řízení a kontroly. Tato pravidla/postupy lze rozdělit na vrcholové (manažerské/řídící) postupy a prováděcí postupy. Při realizovaném outsourcingu navrhujeme posílení kontrolních mechanismů (kontrola parametrů SLA) s dopadem na výši fakturace.

	Poskytovatel outsourcingu	Úřad
Manažerská úroveň	Návrhy, doporučení	Stanovení strategie, rozhodování
Realizační úroveň	Realizace SLA, výkazy, doporučení	Kontrola, řešení změn SLA

V případě interního řešení musí vše zabezpečit úřad.

10.7 FINANČNÍ ODHADY

Konkrétní finanční odhady jsou prováděny z důvodu ocenění Var. 3, tj. pro potřeby plánování zdrojů úřadu pro případ, že by se rozhodl nejít cestou celkového nebo částečného outsourcingu.

Finanční odhady zde vycházejí **z veřejně dostupných informací**. Pro tyto odhady není možno pracovat s možnými předpokládanými slevami, mzdovou politikou úřadu atd. Je tedy kalkulováno s ceníkovými cenami pro koncové uživatele, obvyklými průměrnými platy atd. Tam, kde se jedná o ceny bez a s DPH je koncová cena stanovena s DPH z důvodu sestavování rozpočtu úřadu. V případě kalkulace nákladů na pracovní místo jsou výsledné hodnoty bez DPH.

10.7.1 PERSONÁLNÍ NÁKLADY

Pro personální zabezpečení ve Var. 3 (Interní zajištění) se personální náklady skládají z:

- Mzdových nákladů
- Pojištění mimo sociální a zdravotní, stravenky …
- Nemocenské dávky
- Náklady na vedení personalistiky a zpracování účetnictví
- Náklady na pracovní prostředky, energie, školení …

Pro kalkulaci počtu pracovníků je třeba zohlednit časový rozsah služeb, které musí poskytovat pracovníci úřadu.

Časový rozsah je předpokládán:

- V úřední dny od 8:00 do 19:00
- V neúřední dny od 8:00 do 16:00

Úřední dny jsou Pondělí, středa, čtvrtek. Z toho vyplývá časová náročnost na jeden týden. Úřední den je 11hodin, neúřední den je 8 hodin, za týden toto činí (3 * 11) + (2 * 8) = 49 úředních hodin. Hodiny pracovníka musí být vyšší, neboť svou práci musí zahájit před úředními hodinami a ukončit až po úředních hodinách. S povinnými ½ hodinovými přestávkami je zřejmé, že toto nelze zajišťovat jedním pracovníkem pro požadovaný fix time ani z důvodu dodržení zákoníku práce.

Pro tento časový rozsah je třeba pokrýt následující problematiky v rámci ICT:

V základním rozdělení to jsou:

- Servis HW
- Servis VMWare + OS (Windows, Linux)
- Servis pro SQL servery (Oracle, MS SQL, PostgreSQL, Firebird)
- Servis LAN a aktivní síťové prvky
- Servis pro koncové stanice
- Servis pro správu uživatelských účtů, přístupů, oprávnění
- Help Desk
- Servis pro podporu aplikací/IS a jejich integraci

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Tyto oblasti jsou definovány pro jednotlivé základní problematiky, které je nezbytné řešit pro fungování ICT. Z tohoto důvodu a s ohledem na požadované fix time doporučujeme najímat pouze kvalifikované specialisty pro danou oblast. Pro toto základní rozdělení to jsou minimálně tito specialisté:

- Servisní pracovník HW
- Servisní pracovník VMWare + OS (Windows, Linux)
- Servisní pracovník pro SQL servery (Oracle, MS SQL, PostgreSQL, Firebird)
- Servisní pracovník pro LAN a aktivní síťové prvky
- Servisní pracovník pro koncové stanice
- Servisní pracovník pro správu uživatelských účtů
- Servisní pracovník Help Desku
- Servisní pracovník pro podporu aplikací/IS a jejich integraci

Vzhledem k požadovaným fix time (nejkritičtější jsou do 1hod) je nezbytné, ve stanovených časech, vždy na pracovišti disponovat odpovídajícím specialistou. Vzhledem k týdenní časové náročnosti nelze tyto oblasti pokrýt pouze jedním pracovníkem. Dále je nezbytné počítat s:

- Pracovní neschopností/OČR
- Dovolenou
- Vzděláváním/zvyšováním odbornosti
- Výpovědí
- Úmrtím
- Akcí mimo pracoviště (např. porada na MHMP)
- Služební cestou

Pro tyto nejobvyklejší případy je třeba počítat se zastupitelností pro jednotlivé role. Protože neexistuje jakákoliv garance dostupnosti specialisty pro kombinaci jednotlivých rolí a navíc minimálně dvou stejně kvalifikovaných osob ve zvolené kombinaci, je nezbytné plánovat tuto zastupitelnost v rámci jednotlivých rolí. Pro zajištění var. 3 je třeba, dle našeho doporučení, minimálně 16 (8 rolí * 2) kvalifikovaných pracovníků pro použité technologie a IS.

Pro potřeby úřadu a zastupitelnosti jednotlivých pozic (16ti pracovníků IT) je třeba na každou typovou pozici počítat se dvěma pracovníky (plná zastupitelnost). Ani tento přístup nezaručuje 100% bezvýpadkovost personálu. Typicky jeden **pracovník je na dovolené a druhý onemocní.**

Odhad FTE pro interního koordinátora se liší v závislosti na zvolené variantě.

Pro jednotlivé varianty je odhad následující (včetně zastupitelnosti):

- Var. 1 – 50%
- Var. 2 – 100%
- Var. 3 – 200%

Zde není řešena cena personálu na straně úřadu, který je nezbytný pro všechny tři varianty – tzv. koordinátor. Tuto roli musí zajistit úřad při všech variantách. Zastupitelnost v rámci této role a počet pracovníků se může lišit podle způsobu řešení a způsobu řízení na straně úřadu.

V případě Varianty 3 musí úřad počítat se zajištěním pracovních míst pro jednotlivé pracovníky (kanceláře a jejich vybavení). V případě interního řešení ICT služeb je důsledkem vznik nových pracovních míst.

Pro výpočty byly použity ceny obvyklé na trhu práce, protože tabulkové ceny úřadu nejsou pro trh práce směrodatné a nezaručují získání potřebných odborníků. Tyto výpočty jsou realizovány pro 16 IT pracovníků.

Pro potřeby odhadu mzdových nákladů bylo použito informací ČSÚ (https://www.czso.cz/csu/czso/lidske_zdroje_v_informacni_spolecnosti_it_odbornici (Příloha č. 5) a https://portal.mpsv.cz/sz/stat/vydelky/pra (Příloha č. 6)).

Průměrná mzda vysokoškoláka, specialisty v ICT, je uváděna pro rok 2013na ČSÚ ve výši 53 410,- Kč, zaokrouhleně cca 53 000,- Kč. Na stránkách MPSV je pro rok 2014 tato průměrná mzda uváděna ve výši 57 622,- Kč, zaokrouhleně 58 000,- Kč. Orientační mzdové náklady pro mzdu 58 000,- jsou 77 720,-Kč, zaokrouhleně 78 000,- Kč. Tuto částku na jednoho pracovníka je třeba navýšit o další položky. Tyto další položky kvalifikovaně odhadujeme procentuálně z hrubé mzdy. Tedy:

- Pojištění, mimo sociální a zdravotní, stravenky … (15%)
- Nemocenské dávky (15%)
- Náklady na vedení personalistiky a zpracování účetnictví (1%)
- Náklady na pracovní prostředky, energie, školení … (18%)

Celkem jde tedy o 49% hrubé mzdy, tj. 28 420,- Kč. Lze tedy říci, že personální náklady jsou zaokrouhleně v předpokládané výši 106 000,-Kč/měsíc/pracovníka. V této ceně nefiguruje DPH.

Pro 16 pracovníků na pět let je tato částka 106 000 * 16 * 12 * 5 = **101 760 000,- Kč**.

10.7.2 HW A TECHNICKÁ PODPORA

10.7.2.1 PROBLEMATIKA SWITCHŮ A SÍTĚ LAN

Základní požadavky na aktivní síťové prvky LAN:

- Switch L2, L3
- Min. 48 Ethernet portů (10/100/1000)
- Min 4x 10GB SFP
- Stohovatelnost
- Řízení přístupů na porty (pouze povolená zařízení)
- Provedení rack 19“

Jako referenční ceník jsme použili:

- http://www.router-switch.com/Price-cisco-switches-cisco-switch-catalyst-2960_c19 (viz Příloha 7)
- http://www.globalpricelists.com/globalpricelistcisco.php (viz Příloha 8)

Vhodná zařízení jsou v základním potřebném vybavení v cenách od $3000 do $4500 USD. Při ceně 24,9041 Kč/USD (kurz Komerční banky ze dne 12.8.2015) je toto rozpětí cca 74 720,- až 112 100,- Kč bez DPH za kus.

Pro další odhady budeme počítat s cenou získanou aritmetickým průměrem zjištěných ceníkových cen, tj. 93 410,- Kč bez DPH. Za potřebných 21 ks je to tedy 1 961 610,- bez DPH, tedy 2 373 548,10 Kč s DPH. Při zaokrouhlení na tisíce je to tedy 2 374 000,- Kč.

Technická podpora se obvykle pohybuje ve výši 25% z ceníkové ceny/rok. Servisní programy (např. výměna při závadě do 24 hod. jsou další add platby ročně, obvykle ve výši 10-18% z ceníkové ceny ročně).

Instalační práce, práce na rekonstrukci kabeláže (pokud budou třeba) a případné servisní a re konfigurační práce jsou stanoveny kvalifikovaným odhadem. Tato cena závisí na dodavateli, zjištěné technické situaci a potřebě průběžných změn.

Pro potřeby tohoto odhadu jsou odhadované ceny takovéto:

Položka	Cena v Kč
21 switch dle specifikace	2 374 000,-
Technická podpora na 5 let	2 967 500,-
Add platby – servisní program na 5 let (15%)	1 780 500,-
Instalační a konfigurační práce na 5 let (odhad)	1 190 000,-
Celkem	**8 312 000,-**

Uváděné ceny vycházejí z veřejně dostupných ceníků.

10.7.2.2 FIREWALL

Základní požadavky na firewall:

- Cluster HA
- Antispam
- VPN
- Log analyzer
- Všechny pobočky (centrála + pobočka)

Jako referenční ceník jsme použili:

http://www.insight.com/en_US/buy/partner/fortinet.html?pq=%7B%22priceRangeLower%22%3A0%2C%22priceRangeUpper%22%3A0%2C%22sortBy%22%3A%22BestMatch%22%2C%22searchTerms%22%3A%7B%22FORTINET%22%3A%7B%22field%22%3A%22field%22%2C%22value%22%3A%22A-MARA-MFRNR~0007042037%22%7D%7D%7D

Pro předpokládané řešení bylo zvoleno zařízení s vysokou propustností, ve shodě s vizemi celopražských služeb, pro připojení poboček bylo zvoleno zařízení odpovídající současným standardním požadavkům na propustnost.

U vysoko propustného zařízení ceník uvádí 3letou záruku a režim 7x24, u obvyklého ceník uvádí 2 letou záruku a režim 7x24. Tyto záruky se dají prodlužovat a dokupovat, ale ceník tyto položky samostatně neuvádí. Proto do doby 5 let použijeme aproximaci ceny, kde prodloužení podpory budeme počítat ve výši 25% pořizovací ceny/rok.

Vysoko propustné zařízení: $20000,- na 3 roky + $10000,- na 2 roky = USD $30000,-

Obvyklé zařízení: $6000,- na 2 roky + $4500,- na 3 roky = USD $10500,-

Obě tato zařízení jsou nutná ve dvou kusech pro cluster HA. Použitý kurz je 24,9041 Kč/USD.

Výsledná cena pořízení a technické podpory je tedy ($30000 + $10500)*2*24,9041= 2 017 232,10 Kč, zaokrouhleně na tisíce 2 018 000,- Kč.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Celková částka na pořízení FW je tedy 2 441 780,- Kč včetně DPH.

Služby za servis (konfigurace, update firmware apod.) odhadujeme ve výši 500 000,- Kč na 5 let, celkem tedy v součtu s 2 441 780,- Kč je to 2 941 780,- Kč.

Uváděné ceny vycházejí z veřejně dostupných ceníků.

10.7.2.3 DISKOVÁ POLE + ZÁLOHOVÁNÍ

Základní požadavky na disková pole:

- Rack mount 19“
- Redundance klíčových prvků (napájení, síť …)
- Základní kapacita 20TB a možnost navýšení kapacity
- Podpora virtualizace (VMWare)
- Podpora RAID 0, 1,5,6
- Podpora mirroru celých polí
- Podpora rozšířených funkcí, zejména deduplikace
- Podpora SAN
- Podpora výrobce minimálně 5 let

Disková pole je nutno obnovit, protože výrobce zkrachoval a není možno řešit havarijní stavy.

Pro tento odhad byly použity následující ceníky:

- http://www.dell.com/uk/business/p/storage-sc2000/fs (Příloha č. 10)
- http://www8.hp.com/cz/cs/products/disk-storage/product-detail.html?oid=5386548#!tab=specs (Příloha č. 10)

V těchto cenících je uvedeno pouze šasi bez HDD. Disky jsou samostatnou nákupní položkou. Celkový odhad se tedy skládá z 2x šasi a N x HDD tak, aby raw kapacita byla 25 TB.

Cena odpovídajícího šasi se pohybuje okolo 500 000,- Kč včetně DPH. Jeden disk typu SAS (4TB) určený pro provoz 24x7 se cenově pohybuje okolo 22 000,- Kč s DPH.

Odhadovaná cena je konstruována takto: 2 * 500 000 + 2*(22 000 * 7) = 1 308 000,- Kč včetně DPH.

Technická podpora je odhadnuta ve výši 25%/rok z pořizovací ceny šasi na dobu pěti let, tj. 1 250 000,- Kč včetně DPH.

Celkem pořizovací cena je odhadnuta na 2 558 000,- Kč včetně DPH včetně technické podpory na 5let.

Základní požadavky na zálohování:

- Pásková knihovna
- Výměnné cykly dle plánu
- Podpora SW Backup Exec 2012
- Podpora výrobce minimálně 5 let

Pásková knihovna aktuálně pracuje a zde je nutno pouze řešit technickou podporu včetně zálohovacích médií.

Cena na technickou podporu zálohování je odhadnuta na 720 000,- Kč/5let včetně DPH.

Celková cena za tuto kapitolu je **3 278 000**,- Kč včetně DPH.

Uváděné ceny vycházejí z veřejně dostupných ceníků.

10.7.2.4 SERVERY

Základní požadavky na servery:

- Podpora virtualizace (VMWare)
- Rozšiřitelnost výkonu
- Podpora SAN, iSCSI
- Redundance prvků
- Podpora minimálně clusteru HA
- Podpora výrobce minimálně 5 let

Současný server (Blade chassis) je třeba obnovit a dokoupit takové prvky, aby bylo dosaženo plnohodnotného stavu minimálně na úrovni cluster HA.
Pro tento odhad byly použity tyto ceníky:

- http://www.etb-tech.com/servers/dell-blade-servers/poweredge-m600 (Příloha č. 11)

Server (chassis + blades) je v cenových relacích 900 000,- Kč bez DPH. Technická podpora na 4 roky (první rok je v ceně) je obvykle ve výši 25% z ceníkové ceny, tj. 900 000,- Kč bez DPH. Dále je třeba zakoupit vhodný servisní program, který obvykle bývá ve výši 18% z ceníkové ceny na rok, tj. 810 000,- Kč bez DPH. Příslušné potřebné SAN prvky jsou oceněny odhadem ve výši 500 000,- Kč bez DPH.

Servery s podporou celkem tedy jsou odhadnuty na **3 763 100**,- Kč včetně DPH.

Uváděné ceny vycházejí z veřejně dostupných ceníků.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

10.7.2.5 STANICE PRO PRACOVNÍKY

Ceny zde uváděné jsou získány z alza.cz.

Základní požadavky na pracovní stanice:

- RAM minimálně 8 GB
- Procesor minimálně I5 nebo srovnatelného výkonu
- HDD minimálně 0,5 TB
- OS windows úrovně professional (dle plánu úřadu)
- MS office (dle plánu úřadu)
- Monitor LCD full HD 21“, výškově stavitelný

Rozdělení PC

Určení	Počet ks
Zaměstnanci	390
Učebna	28
Terminály	24
Externí pracovníci	8

Cenová kalkulace PC

Case verze – 21 300,- Kč s DPH

Monitor – 4 000,- Kč včetně DPH

Technická podpora na 5 let je odhadnuta ve výši 15% ročně z ceníkové ceny, tj. 25 300,- Kč na 5 let včetně DPH.

Stanice celkem 44 275,- včetně DPH a technické podpory na 5 let

Celkový současný počet stanic je 450. Výsledná částka potřebná na obnovu je 19 915 650,- Kč včetně DPH.

Základní požadavky na Notebooky:

- RAM minimálně 4 GB
- Procesor minimálně I5 nebo srovnatelného výkonu
- HDD minimálně 0,5 TB
- OS windows úrovně professional (dle plánu úřadu)
- MS office (dle plánu úřadu)
- USB porty pro připojení klávesnice, myši, případně LAN
- Display LCD full HD
- Možnost připojení externího monitoru VGA, HDMI

Ceníkové ceny specifikovaného notebooku jsou v oblasti 18 000,- Kč včetně DPH. Technickou podporu počítáme ve výši 20% z ceníkové ceny na rok, tj. za pět let je to 18 000,- Kč. Celkem cena s technickou podporou na 5 let za jeden kus je 36 000,-Kč včetně DPH. V současné době je provozováno 82 notebooků.

Pro stanovení celkových nákladů provedeme prosté pronásobení ceny a počtu kusů, tj. 2 952 000,- Kč.

Cena celkem za tuto kapitolu je **22 867 650**,-Kč včetně DPH.

Uváděné ceny vycházejí z veřejně dostupných ceníků.

10.7.3 CENY OUTSOURCINGU

Na základě provedeného průzkumu:

- http://info.mironet.cz/sluzby-a-reseni/123-outsourcing-it
- http://www.itpa.cz/cenik/
- http://www.iservices.sk/index.php?id=6
- http://www.vestnikverejnychzakazek.cz/cs-CZ/Form/Display/590352
- https://zakazky.eagri.cz/contract_display_4528.html
- http://www.egov.cz/clanky/registr-vozidel-bude-nove-spravovat-o2-stat-usetri-az-100-milionu
- http://www.egov.cz/clanky/prehled-verejnych-zakazek-z-oblasti-egovernmentu-za-32-tyden-letosniho-roku4066 dole
- http://www.egov.cz/clanky/prehled-verejnych-zakazek-z-oblasti-egovernmentu-za-30-tyden-letosniho-roku4050 dole
- http://www.egov.cz/clanky/prehled-verejnych-zakazek-z-oblasti-egovernmentu-za-25-tyden-letosniho-roku4006 dole
- http://www.egov.cz/clanky/prehled-verejnych-zakazek-z-oblasti-egovernmentu-za-24-tyden-letosniho-roku3999 dole

můžeme konstatovat, že ceny outsourcingu stagnují, v řadě případů klesají.

Na základě tohoto průzkumu je kvalifikovaný odhad cen outsourcingu založen na cenách ukončeného outsourcigu poskytovaného O2.

Výchozí cena outsourcingu O2 je, zaokrouhleně na statisíce, 129 900 000,- Kč bez DPH, tj. 157 179 000,- s DPH 21%.

Pro rozsah je obdobný jako současnému rozsahu, ale bez Call Centra, je použita cena outsourcingu O2 od které je odečtena aktuální cena za Call Centrum (17 700 000,- na 5 let).

Tato cena je tedy 157 179 000 - 17 700 000 = 139 479 000

Pro variantu 1 je takto upravená cena navýšena. Toto navýšení je kvalifikovaně odhadnuto takto:

- Síťové prvky , tj. plus 8mil Kč

Pro Variantu 1 je tedy odhadovaná cena ve výši 147 479 000,- Kč včetně DPH.

Varianta 2 je tvořena kombinací outsourcingu a realizací vlastními silami. Zde je proveden prostý odhad ceny takového outsourcingu, protože nejsou k dispozici porovnatelná ceníková data.

Pro tento odhad použijeme i již výše specifikovanou částku 139 479 000,- Kč, kde jsou zahrnuty balíčky A, B, F, I. Tato částka musí být navýšena o následující položky (interní zabezpečení):

- Obnova LAN sítě
- Náklady na pracovní místa
    - Správce LAN (včetně zastupitelnosti)

- Pracovník bezpečnosti (včetně zastupitelnosti)

K uvedené částce tedy přičteme:

- 8mil – LAN
- 3 pracovníky (2 specialisti LAN, 1 pro ISMS)

  Pro specialistu LAN jsou měsíční náklady odhadnuty, ve shodě s 10.7.1, na 106 000,-Kč/měsíc/osobu. Na 5let je to 12 720 000,- Kč.

  Pro pracovníka ISMS náklady na pracovní místo, kde průměrný hrubý plat odhadujeme na 35 000,- plus odvody 11 900,- plus obdobné náklady jako v kapitole 10.7.1, tj. 17 150,-. Celkem za tohoto pracovníka na 5 let to činí 3 843 000,- Kč na pět let.

Výsledná odhadovaná částka pro variantu 2 je 156 042 000,- Kč.

10.7.4 TECHNICKÁ PODPORA SW

Kalkulace těchto částek vychází z cen za aktuálně poskytované služby.

Ceny služeb v Kč včetně DPH (zaokrouhlena na tisíce nahoru)

Položka	Cena/měsíc	Cena/5let
SW a aplikační podpora	954 000,-	57 240 000,-

Vzhledem k tomu, že provoz Call Centra bude řešen samostatným postupem, není zde oceněn.

10.7.5 POROVNÁNÍ VARIANT

V následující tabulce je provedeno shrnutí cen z jednotlivých oceňovaných kapitol pro účely Var. 3.

Položka	Cena v Kč
Personální náklady	101 760 000
Problematika switchů a sítě LAN	8 312 000
Firewall	2 941 780
Disková pole + zálohování	3 278 000
Servery	3 763 100
Stanice pro pracovníky	22 867 650
Technická podpora SW	57 240 000
Cena celkem	200 162 530

V následující tabulce je uvedeno finanční porovnání jednotlivých variant definovaných v kap. 7, 8 a 9.

Ceny uváděny v Kč.

	Var1	Var2	Var3
Cena	**147 479 000,-**	**156 042 000,-**	**200 162 530,-**

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

V následující tabulce je provedeno porovnání hlavních rizik jednotlivých variant.

Riziko	Var1	Var2	Var3
Technologická dostatečnost	Nízké riziko – parametry SLA	Střední riziko – parametry SLA + vlastní	Vysoké riziko
Výkonová dostatečnost	Nízké riziko – parametry SLA	Nízké riziko – parametry SLA Vysoké riziko u vlastních parametrů	Vysoké riziko
Řízení odstraňování závad	Nízké riziko – parametry SLA	Vysoké riziko	Střední riziko
Nastavení SLA parametrů	Vysoké riziko	Vysoké riziko	Nutnost řešení, vysoké riziko
Nábor personálu	Úřad neřeší	Střední až vysoké riziko	Vysoké riziko
Architektura řešení	Úřad neřeší	U SLA úřad neřeší, Střední až vysoké riziko u vlastních	Vysoké riziko
Určení zodpovědnosti	Nízké riziko – parametry SLA	Vysoké riziko	Střední riziko
Časové riziko	Nízké riziko – parametry SLA	Střední riziko – parametry SLA + vlastní	Vysoké riziko

V následující tabulce je provedeno porovnání plusů a mínusů jednotlivých variant

Var1	Var2	Var3
+ plní smluvní požadavky - možnost kontroly	+ partner plní smluvní požadavky - úřad musí plnit technické závazky	- kontrola plnění požadavků vlastními lidmi (minimální sankce)
- Problematika předčasného ukončení	- Problematika předčasného ukončení	+ není SLA, které by se muselo ukončit
+ úřad neřeší personalistiku	- řešení personalistiky pro interní balíčky	- řešení personalistiky
+ úřad neřeší pracovní prostředky	- řešení pracovních prostředků	- řešení pracovních prostředků a míst
+časový harmonogram – vymahatelnost	- časová připravenost úřadu	- časová připravenost úřadu
- vhodnost parametrů SLA	- vhodnost parametrů SLA	- úřad musí stanovit parametry služeb
+ jedno místo pro řešení problémů	- úřad musí správně a dokladovatelně předávat a řešit tickety (řešit problémy)	- úřad musí správně a dokladovatelně řešit tickety (řešit problémy)

Tyto tabulky jsou shrnutím výsledků a projednávané problematiky s jednotlivými politickými kluby.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

11 ZÁVĚR

Závěrem můžeme rekapitulovat takto:

- Je třeba zahájit zavedení systému řízení za účelem strategického řízení ICT úřadu
- Je třeba zahájit řešení problematiky ISMS a Zákona o kybernetické bezpečnosti
- Je třeba stanovit základní parametry pro jednotlivá definovaná aktiva

V současné době je zejména nezbytné stanovit strategický směr, kudy bude ICT úřadu směřováno dále. Základní směry vyplývají z uvedených tří variant:

- Plný outsourcing
- Částečný outsourcing
- Vlastními silami

Na základě tohoto rozhodnutí je možno přistoupit k dalšímu kroku a společně s úřadem připravit potřebné RfP. Úřad na této přípravě musí participovat zejména při nastavení hodnot parametrů, které jsou nezbytné pro jakoukoli z uvedených variant nebo varianty vzniklé modifikací některé z variant.

12 PŘÍLOHA Č. 1

PRA HA
PRA GUE
PRA GA
PRA G

HLAVNÍ MĚSTO PRAHA
MAGISTRÁT HLAVNÍHO MĚSTA PRAHY
ODBOR INFORMATIKY

MHMPP0545VCK

[redacted]
Městská část Praha 10
Mgr. Ivana Cabrnochová
Vršovická 68
101 38 Praha 10

[redacted]

Váš dopis zn.	Č.j.	Vyřizuje / linka	Datum
	MHMP/1090/2015	**Šolc/2670**	**25.6.2015**

Věc: Odpověď na dotazy k problematice IS/ICT

Vážená paní radní,

tímto sdělením reaguji na Vaše dotazy zaslané dopisem č.j. P10-056571/2015 vztahující se k problematice součinnosti MHMP s městskými částmi a zajištění služeb v oblasti informačních systémů a informačních technologií. Váš zájem byl zaměřen na podporu v oblasti aplikací, konektivity, agendových a ekonomických systémů, licencí, infrastruktury (HW), rozšíření služby Czech POINT atd. Níže uvádím odpovědi na Vaše dotazy ve struktuře, v jaké byly položeny.

1) *Které služby poskytované Magistrátem hl. m. Prahy v rámci podpory v oblasti IS/ICT budou moci městské části využívat?*

   Magistrát hl. m. Prahy pokračuje v zajišťování služeb podporujících činnost MČ v rozsahu zavedeném v minulých letech. Jedná se především o připojení k síti MepNet, zajištění licencí a základní podpory vybraných systémů celoměstského významu (JES/GINIS, Proxio, E-Spis). V případě JES/GINIS je zajištěna podpora do března 2017 na základě JŘBU, což přináší mj. dílčí omezení v rozvoji dle požadavků MČ. Další aktivity jsou realizovány v oblasti metodiky, komunikace a výměny zkušeností.

2) *V jaké podobě, v jakém rozsahu a v jakém časovém horizontu lze případnou podporu očekávat?*

   Výše uvedená podpora je již zajišťována a nepředpokládáme její omezení. Rozvoj formou dalších projektů je uveden dále.

3) *Plánuje či připravuje Magistrát hl. m. Prahy v oblasti IS/ICT nějaké významné celopražské projekty, které by se mohly nějakým způsobem dotýkat i MČ Praha 10?*

   V současné době je stanovena vize dalšího rozvoje IS/ICT v hl. m. Praze pod heslem „Jedno město, jedno ICT“. Základní principy jsou formulovány v Programovém prohlášení Rady hl. m. Prahy na období 2014-2018, dále pak v dokumentech rozpracovávaných Komisí RHMP pro ICT, jejímiž členy jsou rovněž zástupci MČ. V komisi byly již diskutovány některé projektové záměry, které se mohou dotýkat MČ, tedy i Prahy 10, jsou např.

Sídlo: Mariánské nám. 2, 110 01 Praha 1
Pracoviště: Jungmannova 29/35, 110 00 Praha 1
tel. 236 001 111, fax 236 007 150
e-mail: inf@cityofprague.cz

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

- Otevřená data (OpenData) – publikování otevřených dat a rozhraní pro využití a tvorbu aplikací třetími stranami
- Prague Market – vytvoření jednotného kontaktního, objednávkového a platebního místa, které bude pracovat jako zprostředkovatel služeb poskytovaných městem (HMP, MČ, městské organizace).
- Centrální řešení správa uživatelských účtů (Identity Management System)
- Zajištění bezpečnosti sítě MepNet (bezpečnostní perimetr)

Dalšími tématy v jednání jsou: Digitální strategie HMP; Centrální řešení serverů pro elektronickou poštu (Exchange); Centrální řešení služby správy požadavků (Service Desk); Rozvoj agendového systému Proxio; Portál a mobilní služby; Ekonomický systém; Informační systém krizového řízení.

Projekty budou řízeny prostřednictvím řídících výborů, ve kterých budou zastoupeny klíčové zainteresované strany. V případě projektů s dopadem na MČ tak budou zástupci MČ zváni do řídících a realizačních struktur projektů.

4) *Může být MČ Praha 10 nějakým způsobem Magistrátu hl. m. Prahy v oblasti rozvoje IS/ICT nápomocna?*

Může, stejně jako ostatní MČ. Jedná se především o nastavení operativní součinnosti mezi MHMP a MČ v dané tematické oblasti. Považujeme za vhodné určit ze strany MČ kontaktní osobu pro průběžnou odbornou komunikaci, která bude partnerem pro odbor informatiky MHMP. Dále uvítáme zapojení do příprav a realizace nových projektů. Předpokládáme, že budou realizovány nejprve formou pilotních řešení, na základě dobrovolné spolupráce. Teprve následně by měly být rozšiřovány v celopražském měřítku.

5) *Jaký je stav přípravy a realizace Celoměstské koncepce rozvoje informačních systémů pro potřeby hl. m. Prahy a městských částí (s odkazem na § 36 a násl. vyhlášky hl. m. Prahy č. 55/2000 Sb., kterou se vydává Statut hl.. m. Prahy)? Pozn.: původní dotaz nečíslován.*

Dokument Celoměstská koncepce rozvoje informačních systémů pro potřeby hlavního města Prahy a městských částí na období 2013-2016 (Celoměstská koncepce, CMK) byl připraven jako jeden z koncepčních dokumentů z let 2013-2014 právě s ohledem na požadavky Zákona o hl. m. Praze a Statutu hl. m. Prahy. Nicméně, poté co prošel připomínkovým řízením a byl upraven dle akceptovaných připomínek, došlo ke změně v roli odpovědného radního HMP pro informatiku. Dokument byl v roce 2014 znovu posuzován, došlo k dílčím úpravám (úvod a shrnutí) a byl připraven Tisk do RHMP. S blížícím se koncem volebního období však nedošlo k projednání v RHMP, tedy ani ZHMP. Tento stav trvá. Zvažuje se další aktualizace s ohledem na politicky určené priority dalšího rozvoje a na požadavky ze strany městských částí. Každopádně, základní principy součinnosti a standardizace v podmínkách hl. m. Prahy budou uplatňovány i při realizaci jednotlivých celoměstských projektů.

Dovolte mi závěrem poděkovat za Váš zájem o problematiku IS/ICT v celoměstském měřítku. Zároveň bych rád konstatoval, že odbor informatiky MHMP má v úmyslu nadále pokračovat v osvědčené spolupráci a komunikaci

s městskými částmi formou schůzek informatiků, dosud konaných zhruba čtvrtletně. Nadále budeme zajišťovat poskytování aktuálních informací o dílčích tématech i odpovědí na specifické dotazy, a to takovouto oficiální formou dopisu, ale i přímo v kontaktu s jednotlivými odpovědnými odbornými pracovníky odboru. Jsme připraveni poskytovat informace i na jiných setkáních, např. stejně jako na setkání tajemníků MČ, které se uskutečnilo minulý týden. V případě zájmu či nejasností jsem spolu s ostatními pracovníky odboru informatiky připraven poskytnout další informace Praze 10 i jiným městským částem. Věřím, že vzájemná spolupráce je v oblasti IS/ICT základní podmínkou a klíčem k úspěchu.

S pozdravem

Hlavní město Praha
Magistrát hl.m. Prahy
Jungmannova 35/29
111 21 Praha 1 /43/

Ing. Pavel Mánek

ředitel odboru informatiky

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

13 PŘÍLOHA Č. 2

13.1 ODKAZ

http://www.microsoft.com/enterprise/cs-cz/verejna-sprava/statni-sprava.aspx#fbid=ouHjHVSa78g

13.1.1 OBSAH

13.1.1.1 VIZE

Informační systém nemusíte vždy vlastnit, nebo provozovat u sebe na svých vlastních technologiích. Jsou situace a potřeby, kdy pronájem informačního systému je pro vás mnohem výhodnější, než investice do vlastní infrastruktury. Informačním systémem myslíme nejen vaše aplikace, ale i vaše systémové prostředí, ve kterém vaše aplikace provozujete. Místu, kde je pro vás informační systém provozován (a vy platíte jen za jeho užívání), se říká veřejný cloud. Microsoft má pro vás několik cloudových (online) služeb, pomocí kterých si můžete sestavit svůj vlastní informační systém včetně systémového prostředí tak, že ve vaší organizaci v důsledku potřebujete jen počítače pro uživatele a připojení k internetu. Důležité je, že můžete platit jen za to, co skutečně využíváte a spotřebováváte. Cloudové služby by mělo být možné používat v návaznosti na vaše lokálně provozované informační systémy - zejména vyřešit sjednocení identit a přístupových práv s vaším místním adresářem Active Directory tak, aby vaši uživatelé vůbec nepoznali, že pracují v informačním systému, který není fyzicky umístěn ve vašem datovém centru. Dále je pro vás důležité, aby provozovatel cloudových služeb poskytnul dostatečnou ochranu v oblasti bezpečnosti a soukromí dat, což by dle zák. 101/2000 Sb. mělo být ošetřeno ve Smlouvě o zpracování osobních informací mezi správcem a zpracovatelem dat.

13.1.1.2 UKÁZKY ŘEŠENÍ

Kancelář a správa dokumentů jako služba

Microsoft Office 365 je online nástroj, který svoji funkcionalitou vychází z Microsoft Office. Ten je vašim uživatelům velmi dobře znám. Umožní Vám přístup a práci s dokumenty a s poštou odkudkoliv a z jakéhokoliv počítače připojeného k Internetu. V kombinaci s našimi cloudovými službami Microsoft Exchange Online, Microsoft Lync Online a Microsoft Sharepoint Online máte k dispozici prostředí, které vám umožní spolupráci vašich zaměstnanců online, aniž byste museli investovat do vlastní ICT infrastruktury.

Agendové systémy jako služba

Agendový systém postavený na jedné datové a procesní platformě, která může být s výhodou sdílena pro většinu agend zpracovávaných na úřadě, významně šetří vaše finanční finanční prostředky. Pokud se vám nechce investovat do pořízení platformy pro agendový systém, nabízíme vám naše řešení Microsoft CRM Online. Úpravu stávajících a tvorbu nových agend v takovém systému může úřad zvládnout i vlastními silami. Máte tedy všechny výhody platformy pro agendové systémy (podrobnosti v sekci Agendové systémy), ale platíte jen za to, co skutečně potřebujete a používáte.

Infrastruktura a servery jako služba

Pokud dnes provozujete nějaké své informační systémy a aplikace na vlastních serverech a potýkáte se často s nedostatkem místa a výkonu těchto serverů, je pronájem infratsruktury pro provoz informačního systému pro vás správný krok. Microsoft pro tyto účely nabízí online službu Windows Azure. Pronajatou infrastrukturu můžete jednoduše integrovat s vaší vlastní infrastrukturou tak, že to vaši uživatelé, ani vaše informační systémy nepoznají.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

14 PŘÍLOHA Č. 3

14.1 ODKAZ

http://www.reuters.com/article/2014/07/31/us-usa-tech-warrants-idUSKBN0G024I20140731?feedType=RSS

14.1.1 OBSAH

Microsoft Corp must turn over a customer's emails and other account information stored in a data center in Ireland to the U.S. government, a judge ruled on Thursday, in a case that has drawn concern from privacy groups and major technology companies.

Microsoft and other U.S. companies had challenged the warrant, arguing it improperly extended the authority of federal prosecutors to seize customer information held in foreign countries.

Following a two-hour court hearing in New York, U.S. District Judge Loretta Preska said a search warrant approved by a federal magistrate judge required the company to hand over any data it controlled, regardless of where it was stored.

"It is a question of control, not a question of the location of that information," Preska said.

The judge said she would temporarily suspend her order from taking effect to allow Microsoft to appeal her decision to the 2nd U.S. Circuit Court of Appeals.

The case appears to be the first in which a corporation has challenged a U.S. search warrant seeking data held abroad.

A number of technology companies filed court briefs in support of Microsoft's position, including AT&T Inc, Apple Inc, Cisco Systems Inc and Verizon Communications Inc.

The companies are worried that they could lose billions of dollars in revenue to foreign competitors if customers fear their data is subject to seizure by U.S. investigators anywhere in the world.

Thursday ruling concerns a search warrant served on Microsoft by prosecutors for a customer whose emails are stored in a data center in Dublin, Ireland.

It is unclear which agency issued the warrant because the warrant and all related documents are sealed.

The technology companies argued that U.S. search warrants cannot be executed overseas under the law. But lawyers for the U.S. Justice Department said the warrant only required the company to provide documents it controls, just as U.S. banks can be forced to hand over transaction records held in foreign countries.

(Editing by Grant McCool)

15 PŘÍLOHA Č. 4

15.1 ODKAZ

https://www.eff.org/files/2014/06/12/att_amicus_brief_in_support_of_microsoft_re_extraterritorial_search_warrant.pdf

15.1.1 OBSAH

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION	13 Mag. 2814

MEMORANDUM OF LAW OF *AMICUS CURIAE* AT&T CORP. IN SUPPORT OF MICROSOFT CORPORATION

Charles W. Douglas*
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000
cdouglas@sidley.com
* *Of Counsel*
Attorneys for AT&T Corp.

Alan Charles Raul
Kwaku A. Akowuah
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000
araul@sidley.com
Attorneys for AT&T Corp.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICUS

Amicus curiae AT&T Corp., together with its affiliates (collectively, "AT&T"), is one of the world's largest providers of telecommunications and information services, and as a result frequently engages with law enforcement officials about ongoing investigations. As set forth in a recent "transparency report," AT&T receives numerous demands for information in relation to civil and criminal matters from federal, state and local law enforcement agencies in the United States.[1] As it must, AT&T complies with the Stored Communications Act (SCA) in responding to those demands. In addition, AT&T received a number of requests last year from foreign law enforcement agencies for information that is stored in the United States.[2] AT&T refers such international requests to the applicable Mutual Legal Assistance Treaty (MLAT) process for the requesting country.[3] Pursuant to that MLAT process, AT&T works with the Federal Bureau of Investigation to ensure that any resulting data transfer occurs pursuant to a warrant or other form of process specified by the SCA, and is otherwise consistent with U.S. law. This practice rests on an understanding that when it comes to data storage and privacy protections, location matters. AT&T and AT&T's domestic operating affiliates have relationships with millions of individual U.S. persons and businesses that are rooted in the United States, where their data also sits. U.S. law should govern access to that data. Like other multinational information service providers, AT&T also has business relationships with non-U.S. persons, and in many such cases, access to

---

[1] *See* AT&T Transparency Report, *available at* http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html.
[2] *See id.*
[3] AT&T's understanding is that other U.S. companies, including Verizon, Apple, and Facebook, have adopted similar practices. *See* Verizon Transparency Report, available at http://transparency.verizon.com/international-data; Facebook Information for Law Enforcement Authorities, *available at* https://www.facebook.com/safety/groups/law/guidelines/; Apple Report on Government Information Requests, *available at* http://images.apple.com/pr/pdf/131105reportongovinforequests3.pdf, at 3 n.2 (Nov. 5, 2013).

the relevant data should not necessarily be governed by U.S. law – even though the data may be technically accessible to AT&T in the United States.

The decision reached by Magistrate Judge Francis is troubling because it makes the provider's status as a U.S. entity the only factor relevant to whether U.S. authorities may use U.S. procedures to require disclosure of customer information. Under that approach, a court would not consider, for example, whether the relationship between the customer and provider is centered abroad, whether the customer has any tie to the United States apart from a relationship with an information service provider, or whether foreign law imposes different or additional data protections. AT&T believes that approach is inconsistent with bedrock principles of statutory construction, including the presumption against extraterritoriality. The nationality of the provider cannot be the only factor that determines whether an application of U.S. law is extraterritorial, because that approach disregards factors fundamental to any practical analysis of whether in a particular case, U.S. law is reaching for "data" that is fundamentally foreign. The Court should instead ask whether, considering all relevant factors, the relationship between the provider, the customer and the data at issue has a substantial nexus to the United States.

That analysis may in some circumstances be difficult to perform, precisely because modern information technology practices do not always map easily onto traditional notions of geography. *See Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 168–69 (S.D.N.Y. 1997). But it is no answer to say, as the magistrate judge did, that *all* information that as a technological matter could be accessed from the United States therefore should be treated as subject to U.S. law enforcement demands. That conclusion would transform the SCA's warrant provisions into a global information access tool without bounds. There is no indication that Congress intended the SCA to have that sort of sweeping extraterritorial application. Indeed, the contrary is true –

there is every indication that Congress intended the scope of search warrants to be limited to material that is already grounded in the United States at the time the warrant is issued. This Court accordingly should reject the interpretation adopted by Magistrate Judge Francis.

If the Court does not accept that position, however, it nonetheless should hold that considerations of international comity limit the circumstances in which a warrant should issue for information stored abroad. By any measure, governments have a strong interest in ensuring that their communications privacy and other data protection laws govern relationships between providers and customers that are fundamentally rooted within their borders. Many customers will share a similar expectation that familiar local laws ordinarily will control whether government investigators or others may access their accounts. These and other competing interests ordinarily are addressed through MLAT procedures, which effectively convert a foreign law request for information into a request that conforms to the domestic law requirements of a second country. As such, where the United States has ratified an MLAT applicable to the country where the requested information is stored, the government ordinarily should be required to use the procedures set out in those treaties to obtain the information that it seeks. In other circumstances, the government should be required to make some showing that it cannot satisfactorily obtain the needed information by coordinating with appropriate foreign authorities.

AT&T is concerned that a contrary result could be viewed as a sign that neither the Congress, nor the Executive Branch, nor the courts of the United States respect the data privacy and information law interests of other countries. Given basic notions of reciprocity, that result could work significant harm to U.S. consumers, who rely on an analogous understanding that U.S. privacy and consumer protection laws, rather than foreign laws, control access to data that is stored in this country and does not have a substantial nexus to any other. The Electronic

Communications Privacy Act, which includes the SCA, contains numerous substantive and procedural limitations, as well as transparency, due process and litigation rights, that are not necessarily replicated in foreign laws.[4] U.S. data privacy interests would thus be prejudiced if the magistrate judge's ruling were generalized internationally, and other countries demanded production of all data stored in the United States whenever such data was technically accessible by affiliates subject to foreign jurisdiction. In any event, U.S. businesses could face a significant competitive disadvantage if U.S. law enforcement access to foreign-located data were perceived as unrestrained and disrespectful of foreign interests.

INTRODUCTION

No one doubts that in the Internet Age, information stored by communications providers often is pivotal in law enforcement investigations. For that reason, although the SCA's general purpose is to protect the privacy of electronic data, the statute also requires providers to disclose information about a wire or electronic communication to appropriate government authorities when presented with a warrant, court order, or subpoena, as appropriate. *See* 18 U.S.C. §2703. As relevant here, the SCA authorizes government officials to compel disclosure of content information by obtaining "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." *Id.* §2703(a); *id.* §2703(b)(1). It is undisputed that the SCA does not in express terms mandate compulsory access to information that foreign customers

[4] *See* Vodafone Law Enforcement Disclosure Report, *available at* http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html. ("Laws designed to protect national security and prevent or investigate crime vary greatly between countries, even within the EU…. All countries have a wide range of domestic laws which govern how electronic communications networks must operate and which determine the extent to which law enforcement agencies and government authorities can intrude into or curtail privacy or freedom of expression.... However enacted, these powers are often complex, opaque and convoluted.").

maintain with providers for commercial or personal use outside the United States. In fact, as Magistrate Judge Francis observed, the legislative history of the SCA states that the Act was "intended to apply only to access within the territorial United States." *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 13 Mag. 2814, 2014 U.S. Dist. LEXIS 59296, at *20 (S.D.N.Y. Apr. 25, 2014) (hereinafter "MJ Op.") (quoting H.R. Rep. 99-647, at 32-33 (1986)).

The magistrate judge nonetheless held that a "warrant issued" by him, "using the procedures described in the Federal Rules of Criminal Procedure," compels Microsoft to disclose content information that is stored on servers located in Ireland, no matter where Microsoft's relationship with the customer at issue actually is centered, or where services for that customer are performed. *Id.* at *12. Moreover, he did so without requiring any showing from the government that it has attempted in this case to utilize appropriate MLAT procedures, and without otherwise ensuring that the order is consistent with international comity principles. That conclusion is incorrect for at least three reasons.

First, this decision is inconsistent with the presumption against extraterritoriality. That canon of construction seeks to minimize conflicts between U.S. and foreign law by requiring courts to apply statutes only to domestic matters unless Congress has provided a "clear indication" that the statute also should operate extraterritorially. *See, e.g.*, *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010). The magistrate judge appeared to agree with Microsoft that the SCA does not contain any such "clear indication," but held that this case does not involve an extraterritorial application solely because Microsoft is technically capable of retrieving the data from Ireland using computers here in the United States. MJ Op. at *27–28, 33. That holding is overly simplistic. A New York bank might well have the technical capacity

to transfer funds from a Dublin branch to Manhattan at a keystroke. But it would be implausible to say that act has no effect outside the United States, or that a U.S. law requiring a bank to move funds from Dublin to New York would have no extraterritorial application. This case may well be similar, although AT&T does not have access to sealed information that the parties have provided the Court. In general terms, however, mere technical access is an inappropriate standard because, given modern technology, vast amounts of data could be accessed from almost anywhere from a technical standpoint. And because multinational companies are subject to legal process in many locations, a technical access standard would make their customer data subject to search in places that do not have any connection at all to the customer or to the customer relationship. Put more concretely, the technical access standard endorsed by the magistrate judge has a clear potential to alter the status of information that not only is in Ireland, but has been created as part of a relationship between Microsoft and its customer that does not have a substantial nexus to the United States. Currently, it is held in confidence by Microsoft in Ireland. If the order takes effect, that same information will be transferred to the United States for review by U.S. authorities. Absent facts suggesting that the customer relationship giving rise to that storage has a substantial nexus to the United States (such as that the customer resides in the United States, the customer accesses the data in the United States, or the customer obtains substantial processing or other relevant services in the United States), a U.S. law that requires that transfer to the United States plainly would operate extraterritorially and tread on matters of concern to Irish law. *See* Restatement (Third) of Foreign Relations Law of the United States ("Restatement") §402(1)(b) (1987) (generally, "a state has jurisdiction to prescribe law with respect to … interests in things, present within its territory"); *id* §473(1) ("a state may determine the conditions for taking evidence in its territory in aid of litigation in another state").

Second, the magistrate judge failed to recognize that far from plainly authorizing extraterritorial applications, the statute affirmatively indicates that the statute's warrant provisions are territorially bounded. That textual restriction lies in the word "warrant" itself: When a statutory term like "warrant" has been "obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it." *Sekhar v. United States*, 133 S. Ct. 2720, 2724 (2013). And here that "old soil" includes the unbroken historical tradition that warrants issued by U.S. judges do not run to other countries.

Third, even if a warrant may reach truly extraterritorial circumstances, the magistrate judge erred in failing to qualify his sweeping ruling by applying international comity principles. Even a statute that plainly authorizes some extraterritorial applications must be interpreted so as to avoid unnecessary international friction. *See F. Hoffmann-La Roche Ltd. v. Empagran S.A.*, 542 U.S. 155, 165-66 (2004). Consistent with that principle, it is well established that when a subpoena seeks overseas compliance, a court should not enforce the subpoena without undertaking a case-specific analysis that is sensitive to the comity implications of the information demanded. *See United States v. First Nat'l City Bank*, 396 F.2d 897 (2d Cir. 1968). If the Court accepts the government's counter-textual position that under the SCA, a "warrant" is in essence a subpoena, it should accordingly apply a similar comity analysis in deciding whether to issue or enforce a warrant for information that is stored outside the United States.

ARGUMENT

I. The SCA Does Not Authorize U.S. Courts To Issue Warrants Requiring Providers To Disclose Information Stored In A Foreign Country Absent A Substantial Nexus To The United States.

A. The Presumption Against Extraterritoriality Controls This Question.

"When a statute gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255. This canon of statutory construction, vital in our interconnected world, embodies a "presumption that United States law governs domestically but does not rule the world," (quoting *Microsoft Corp. v. AT&T Corp.*, 500 U.S. 437, 454 (2007)) and "helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013). Its application does not turn on a judicial understanding of a statute's purposes or the policy implications of a strictly territorial reading. Rather than "divin[e] what Congress would have wanted if it had thought of the situation before the court," judges must "apply the presumption in all cases, preserving a stable background against which Congress can legislate with predictable effects." *Morrison*, 561 U.S. at 261.

This principle governs the present dispute between Microsoft and the government. Under 18 U.S.C. §2703(a), a State or federal entity may compel "a provider of electronic communications services" to disclose the "contents of a wire or electronic communication, that has been in electronic storage in an electronic communications system," but only "pursuant to a warrant issued … by a court of competent jurisdiction." A related SCA provision, 18 U.S.C. §2703(b), similarly permits compelled disclosure of content information that is "held or maintained" by "a provider of remote computing service" so long as "the governmental entity obtains a warrant issued" by an appropriate State or federal court.

Nothing in these provisions speaks expressly to whether this "warrant" authority may be exercised with respect to information that is "in electronic storage in an electronic communications system" outside the United States, *id.* §2703(a), or "held or maintained" abroad by a remote computing service. *Id.* §2703(b)(2). Similarly, these provisions do not indicate how

a court should proceed if foreign law imposes different or additional requirements with respect to disclosure. *Cf. E.E.O.C. v. Arabian Am. Oil Co.*, 499 U.S. 244, 256 (1991) ("It is also reasonable to conclude that had Congress intended Title VII to apply overseas, it would have addressed the subject of conflicts with foreign laws and procedures."). There is simply *no* textual indication that Congress intended these warrant provisions to control access to customer accounts that have no substantial relationship to the United States. And because the SCA consequently "gives no clear indication of an extraterritorial application, it has none." *Morrison*, 561 U.S. at 255.[5]

The magistrate judge nonetheless reasoned that "the concerns that animate the presumption against extraterritoriality simply are not present" because "an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data is stored. At least in this instance, it places obligations only on the service provider to act within the United States." MJ Op. at *28.

Respectfully, that is an inadmissibly narrow conception of the presumption, which the Supreme Court has applied to resolve questions as diverse as whether the Attorney General must apply statutory protections for asylum seekers to persons interdicted on the high seas, *see Sale v. Haitian Centers Council, Inc.*, 509 U.S. 155, 173-74 (1993), whether the Federal Tort Claims Act authorizes suits against the United States for allegedly negligent conduct in Antarctica, *see Smith v. United States*, 507 U.S. 197, 203-04 (1993), and whether a federal statute entitled

[5] Indeed, Magistrate Judge Francis tacitly conceded (as has the government) that under the SCA, warranted searches are tied to U.S. interests in at least one respect: They may be directed only to U.S.-based providers. *See* No. 13 Mag. 2814, Dkt. No. 97, Govt' Mem. In Opposition to Microsoft's Motion to Vacate Email Account Warrant at 6 (S.D.N.Y. Apr. 25, 2014) ("Govt Opp.") (SCA "empowers courts to compel service providers *in the United States* to produce records.") (emphasis added)). *See also* MJ Op. at *21–23 (similar conclusion). Neither the magistrate judge nor the government explained why the SCA should be read as requiring that tie to the United States, but *only* that tie.

American private contractors to overtime pay for work performed overseas under contracts with the United States. *See Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949). In each instance, the statute at issue could have been implemented by persons acting within the United States, but that consideration did not affect the Supreme Court's analysis. Rather, the canon rests on a generally applicable "perception that Congress ordinarily legislates with respect to domestic, not foreign matters," *Morrison*, 561 U.S. at 255, and "serves to protect against unintended clashes between our laws and those of other nations which could result in international discord." *Kiobel*, 133 S. Ct. at 1664 (quoting *Arabian Am. Oil Co.*, 499 U.S. at 248). That sort of clash can occur whether or not a statute imposes criminal liability or requires a U.S. citizen to travel overseas. Thus, what matters is whether in practical application, the law regulates foreign matters. That is why the Supreme Court held in *Morrison* that the Securities Exchange Act would operate extraterritorially if a plaintiff could win damages by claiming that a false statement made in Florida caused him to trade to his detriment on an Australian stock exchange. The plaintiff contended that such a suit would only regulate conduct in Florida, but the Supreme Court rejected that position, observing that the suit would also amount to an extraterritorial regulation of the foreign exchange. *See Morrison*, 561 U.S. at 266–67. Likewise, the SCA would in practical effect regulate foreign conduct under the sweeping reading given to the statute by the magistrate judge, because it would govern access to the account of even an Irish customer who had never set foot in the United States, sent data to the United States, or accessed his, her or its data from the United States. Any such application would be quintessentially extraterritorial, even if a provider could facilitate government access by taking technical steps solely within this country. *See United States v. Gorshkov*, No. CR00-550C, 2001 WL 1024026, at *3 (W.D.

Wash., May 23, 2001) (remote search of Russian computer occurred in Russia even though searching officials acted from U.S.).

The government offered a different rationale for evading the presumption. It suggested that the presumption should not apply in this case because Microsoft "structured its affairs in order to place records beyond what it understood to be the reach of U.S. law enforcement." Govt Opp. 19. The magistrate judge did not credit that accusation, instead citing record evidence that Microsoft placed servers abroad for technical reasons that reflect basic properties of physics. MJ Op. at *3. But in any event, the Second Circuit has already made clear that intent evidence is "entirely irrelevant" to the presumption, *United States v. Vilar*, 729 F.3d 62, 78 n.12 (2d Cir. 2013), because a "statute either applies extraterritorially or it does not." *Id.* at 74 (citation omitted). And because the SCA does not contain a "clear indication" that its warrant provisions apply extraterritorially, they do not.

The question that follows is whether the specific application of the statute endorsed by the magistrate judge is extraterritorial, and thus beyond the scope of the statute. As the Supreme Court has noted, it is "often" the case that the presumption "is not self-evidently dispositive, but its application requires further analysis" to determine what is, and is not, a forbidden extraterritorial application. *Morrison*, 561 U.S. at 266. The requisite analysis looks to the "focus" of a statute, namely, the "objects of the statute's solicitude," and what the statute "seeks to regulate." *Id.* at 266-67. The SCA's "focus," as its text repeatedly reflects, is on regulating access to and disclosure of "subscriber or customer" information that is held by providers. *See, e.g.*, 18 U.S.C. §§ 2702, 2703, 2704, 2705. Accordingly, when requested information is stored outside the United States, the extraterritoriality inquiry should turn on whether there is a substantial reason to believe that the regulated relationship between the provider and the

customer or subscriber has a sufficient nexus to the United States. *Cf. Murray v. Schooner Charming Betsy,* 6 U.S. (2 Cranch) 64, 121–22 (1804) (U.S. law would not apply to foreign-flagged ship absent "substantial reason" to believe ship had sufficient American ties); Restatement §403(2) (setting out numerous, case-specific factors for determining when application of U.S. law abroad would be "unreasonable" and therefore inconsistent with international law despite existence of some connection to the U.S.). Frequently, that inquiry will be straightforward, as where a customer resides in one country and contractually or predominantly accesses its account from that country. At other times it will be somewhat complex, such as when a multinational company purchases cloud services for the purpose of regularly accessing data from several countries. Nonetheless, that fact-specific analysis not only squares with *Morrison*, but also avoids the sweeping and unwarranted consequences of the approach adopted by the magistrate, which concludes that any customer relationship that Microsoft may maintain with any customer anywhere in the world is necessarily governed by U.S. law. Congress nowhere indicated that the SCA's warrant provisions should sweep so broadly, and this Court should not adopt that construction.

B. Congress's Choice Of The Word "Warrant" Underscores That Congress Did Not Intend These Provisions To Have Global Scope.

A second interpretive canon further demonstrates that the SCA's warrant provisions do not authorize compelled disclosure of information that lacks a substantial nexus to the United States. That canon holds that when "a word is obviously transplanted from another legal source, whether the common law or other legislation, it brings the old soil with it." *Sekhar*, 133 S. Ct. at 2724 (quoting F. Frankfurter, *Some Reflections on the Reading of Statutes*, 47 Colum. L. Rev. 527, 537 (1947)). That is, "where Congress borrows terms of art" from one legal context, courts presume unless "otherwise instructed" that the new statute "adopts the cluster of ideas that were

attached to each borrowed word in the body of learning from which it was taken." *Id.* (quoting *Morissette v. United States*, 342 U. S. 246, 263 (1952)).

This rule of construction has obvious application to the SCA, which borrowed the word "warrant" from the Fourth Amendment and its common-law predecessors, in keeping with the congressional purpose to "provide a set of Fourth Amendment-like protections for computer networks." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004). It follows that the word "warrant" must be construed consistently with the "cluster of ideas" that surrounds the law of warrants. And as Microsoft has demonstrated (without dispute from the government or the magistrate judge) that body of law has long incorporated a fixed understanding that U.S. courts do not possess global warrant authority. *See, e.g.*, *United States v. Odeh*, 552 F.3d 157 (2d Cir. 2008); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 275 (S.D.N.Y. 2000).

The magistrate judge did not apply this canon because he concluded that the SCA is "ambiguous" with respect to whether the term "warrant" was meant to incorporate "limitations on the territorial reach of a warrant." MJ Op. at *13. But of course, the very purpose of a canon of construction is to resolve uncertainties about how to read a statutory text. *See, e.g.*, *United States v. Colasuonno*, 697 F.3d 164, 173 (2d Cir. 2012). Rather than relying on notoriously fickle guides to legislative intent like inferences drawn from ambiguous statements in the legislative history (MJ Op. at *19–22) or "practical considerations" of policy (MJ Op. at *23–27), the magistrate judge should have accepted that the "warrant" provisions were not intended to apply to every customer account maintained by a U.S. service provider anywhere on earth.

The magistrate judge also declined to give the word "warrant" its ordinary meaning because he concluded that an "SCA warrant" is not a true warrant, but a "hybrid: part search

warrant and part subpoena" that is "obtained like a search warrant" and "executed like a subpoena." MJ Op. at *16. From this, the magistrate judge appeared to conclude that a warrant's application to foreign data is an aspect of the warrant's execution, and that the line of cases requiring subpoena recipients to deliver all responsive materials under their control, no matter where located, accordingly governs interpretation of the word "warrant." MJ Op. at *15–17.

This approach is flawed in several respects. First, and most fundamentally, Congress did not say that it was creating a "hybrid." What Congress said is that a "warrant" must be obtained, and that it must be obtained in the usual way, under the same "procedures" ordinarily used to procure a warrant. What that language most naturally conveys is that the "warrant" described in the SCA is an *ordinary* warrant, not some new griffin-like creation. *Cf. United States v. Bach*, 310 F.3d 1063, 1066 n.1 (8th Cir. 2002) ("While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants [in the SCA] and we find that Congress intended them to be treated as warrants."). Second, even under the magistrate judge's "hybrid" conception, an "SCA warrant" is akin to a conventional warrant in the relevant sense. The question here is whether Congress gave courts power to issue a warrant that operates extraterritorially to compel disclosure of foreign information. That is very much a question about what kind of order the government can obtain. Any question of execution is secondary.

Below, the government likewise argued that an SCA warrant must apply extraterritorially because (1) subpoenas may be enforced in some circumstances with respect to information located abroad, and thus (2) any other view would "conflict with the SCA's general principle that information available through less rigorous legal process is also available through more demanding process." Govt Opp. 8. To be sure, courts have held that federal subpoenas may

apply extraterritorially where that effect is consistent with international comity principles, *see, e.g.*, *First Nat'l City*, 396 F.2d at 901-02, but that does nothing to establish that under the SCA, the same must also be true of a warrant. The government has not cited any authority for the view that if one part of a statute applies extraterritorially, related provisions must likewise apply extraterritorially to maintain purported "structural" consistency. That is no doubt because the Supreme Court has said the opposite is true. *See, e.g.*, *Morrison*, 561 U.S. at 265 ("when a statute provides for some extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms"); *Microsoft v. AT&T*, 550 U.S. at 455-56 (similar).

There is also nothing anomalous about the idea that the SCA's "warrant" provisions would be limited in ways that do not necessarily apply to other related provisions. Under the SCA, the target of a warranted search ordinarily will not have any opportunity to contest the warrant's validity before the search occurs. In contrast, the subpoena provisions of the statute require "prior notice … to the subscriber or customer," 18 U.S.C. §2703(b)(1)(B), and thus offer the person whose account is affected an opportunity to respond, including by seeking judicial intervention. It would not likely have been lost on Congress that allowing U.S. courts to compel delivery of foreign content information without giving prior notice to an affected foreign citizen or government could provoke significant resistance from other countries. For that reason, it would not be surprising in the least if Congress decided to draw the line at subpoenas. Nothing in the text of the statute indicates otherwise.

II. Any Extraterritorial Application Of The SCA's Warrant Provisions Must Be Consistent With Principles Of International Comity.

The magistrate judge's decision is also flawed in a third, independent respect. In sweeping fashion, the ruling directs Microsoft to disclose any and all account information within the four corners of the warrant without regard to whether doing so would violate any substantive

or procedural law of Ireland or whether that information could be obtained through other channels, such as an MLAT request. If the Court concludes that the magistrate judge was right as an initial matter to hold that the SCA authorizes the use of U.S. warrants to compel disclosure of fundamentally foreign material, it should correct that aspect of the decision below.

For decades, courts in the Second Circuit and elsewhere have recognized that cross-border discovery demands in criminal and civil cases can raise serious international comity concerns because nations frequently have "diametrically opposed positions with respect to the disclosure of a wide range of information." *First Nat'l City Bank*, 396 F.2d at 901. That is certainly true where data privacy is concerned – many countries, including nations of the European Union, have adopted conceptions of data privacy interests that differ in some respects from those reflected in American law. *See, e.g.*, Schwartz & Solove, *Reconciling Personal Information in the United States and European Union*, 102 Cal. L. Rev., at *3-5 (Sept. 6, 2013) (forthcoming, *available at* http://ssrn.com/abstract=2271442); Resolution & Report of the American Bar Association, No. 103, at 2-6 (Feb. 6, 2012) (describing differing approaches and calling on U.S. courts to "consider and respect, as appropriate, the data protection and privacy laws of any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation"). As such, there is a clear risk that an unwarranted, unduly aggressive and extraterritorial application of the SCA will produce conflicts with foreign data privacy laws. In such a circumstance, consistent with the understanding of the Founding Generation that our government should accord a "decent Respect to the Opinions of Mankind," *see* Declaration of Independence ¶ 1 (U.S. 1776), international comity principles dictate that "each nation should make an effort to minimize the potential conflict flowing from their joint concern with the prescribed behavior." *First Nat'l City*

Bank, 396 F.2d at 901. Where "a subpoena is directed at information abroad," courts in the Second Circuit typically address that risk of conflict by examining four factors relevant to "whether to order compliance or excuse it." *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 553-54 (S.D.N.Y. 2002). These factors are "(1) the competing interests of the nations whose laws are in conflict, (2) the hardship of compliance on the party or witness from whom discovery is sought, (3) the importance to the litigation of the information and documents requested, and (4) the good faith of the party resisting discovery." *Id.* at 554. The Supreme Court has likewise described a similar list of factors, notably including "whether the information originated in the United States," and "the availability of alternative means of securing the information," as being "relevant to any comity analysis." *See Société Nationale Industrielle Aérospatiale v. United States Dist. Court for the S. Dist. of Iowa*, 482 U.S. 522, 544 n.28 (1987); *see also* Restatement §442(1)(c).

The magistrate judge considered none of these factors – perhaps due to his conclusion that the warrant "places obligations only on [Microsoft] to act within the United States." MJ Op. at *28. But as previously noted, applying the warrant to information now stored in Ireland plainly would implicate interests in Ireland, even if Microsoft ultimately were to transmit the information using a computer located in the United States. It also bears emphasis that the government's argument is in essence that the warrant issued by the magistrate judge should be viewed as a subpoena. If the government prevails on that point, it should have no ground to object to applying a comity analysis drawn from the law of subpoenas.

Thus, if the Court finds that a warrant obtained under the SCA can be used extraterritorially to compel disclosure of foreign data, and if an objection were timely raised that disclosure of the information sought by the United States would conflict or compete with

applicable foreign law, the magistrate judge should consider the case-specific comity implications of the government's demand, and decide on that basis "whether to order compliance or excuse it." *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d at 554.

Consistent with the Supreme Court's statement in *Aérospatiale* that "the availability of alternative means of securing the information," is "relevant to any comity analysis," 482 U.S. at 544 n.28, one other factor should take on special importance in this and future cases of this kind: if the information sought by the government is stored in a country that has an MLAT with the United States, the government ordinarily should be required to rely on MLAT procedures, rather than the SCA, to obtain information from a provider's computer systems. The reason is straightforward. MLAT are binding treaties of the United States, adopted by the President with Senate advice and consent for the precise purpose of addressing the comity concerns (and other logistical obstacles) that cross-border law enforcement investigations frequently present. *See generally*, S. Exec. Rep. 110-13, *Mutual Legal Assistance Treaties with the European Union*, 2-4 (Sept. 11, 2008) (describing the general operation and purposes of MLATs), *available at* http://www.foreign.senate.gov/imo/media/doc/executive_report_110-131.pdf. When the United States seeks to side-step its own mutually negotiated agreement in favor of unilateral action, it is fair for a court to wonder why, and as such, to adopt a rebuttable presumption that unilateral action under the SCA is inconsistent with international comity principles.

This rebuttable presumption would dovetail with the approach that many American providers have adopted for addressing analogous information requests from foreign law-enforcement officials. As explained, AT&T and other major American providers do not respond directly when foreign governments request information that is stored on servers in the United States, and instead refer the requestors to the MLAT process. *See supra* at 1. That policy serves

several interlocking purposes. First, it gives U.S. persons assurance that every disclosure made to law-enforcement authorities will be made consistent with U.S. legal standards, no matter whether the request comes from a domestic or foreign government. Second, the policy affords U.S. authorities an opportunity to intervene if the foreign request raises any issue of U.S. law or policy. And third, the policy helps providers avoid "conflicting commands" from multiple sovereigns, *First Nat'l City Bank*, 396 F.2d at 901, because the MLAT process brings the sovereigns together to discuss how the provider should address the law-enforcement request.

If sustained, the approach adopted by the magistrate judge could unsettle that salutary policy. The reason is simple: under that approach, the law of the foreign place where data is stored is irrelevant to whether the provider must disclose information to U.S. authorities. If courts in this country adopt that approach, it seems safe to predict that foreign officials will likewise seek to forgo the MLAT process and demand that U.S. providers allow access to U.S.-based servers when presented with orders that satisfy foreign law.[6]

The approach adopted by the magistrate judge also poses a serious risk of harm to American companies. As the Court is no doubt aware, the scale and reach of U.S. government surveillance has been a subject of considerable controversy, and substantial misunderstanding, in recent years. That controversy has prompted some to argue that foreign consumers should not entrust their information to U.S.-based firms because of a misimpression that the U.S. government has inordinate and undue access to the information that these companies possess. *See, e.g.*, Kashmir Hill, *How the NSA Revelations Are Hurting Businesses*, Forbes Magazine (Sept. 10, 2013), *available at* http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/; *Foreign Intelligence Surveillance Act (FISA) Reforms:*

[6] *See* Vodafone Law Enforcement Disclosure Report, *supra* at 4 n.4.

Hearing Before S. Select Comm. on Intelligence, 112th Cong. (Comm. Print 2014) (statement of Dean C. Garfield, President & CEO, Information Technology Industry Council), *available at* http://www.intelligence.senate.gov/140605/garfield.pdf. A decision like the one reached by the magistrate judge can only feed that unfortunate perception, because its bottom-line holding appears to be that under the SCA, U.S.-based providers alone may be compelled to give U.S. authorities access to information held anywhere in the world, without regard to applicable foreign law or whether the customer-provider relationship has any substantial nexus to the United States. This Court should not endorse that view, which risks placing U.S. providers at a significant competitive disadvantage in foreign markets.

CONCLUSION

For the foregoing reasons, this Court should conclude that the SCA does not authorize U.S. courts to issue warrants that operate extraterritorially to compel providers to disclose foreign information lacking a substantial nexus to the United States. Alternatively, if the Court concludes otherwise, it should require the magistrate judge to conduct an international comity analysis before deciding whether the warrant in this case should be enforced in respect to information stored in Ireland.

Dated: June 11, 2014

Respectfully submitted,

/s/ Alan Charles Raul

Charles W. Douglas*
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000
cdouglas@sidley.com
* *Of Counsel*
Attorneys for AT&T Corp.

Alan Charles Raul
Kwaku A. Akowuah
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000
araul@sidley.com
Attorneys for AT&T Corp.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION	13 Mag. 2814

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Civil Procedure 7.1 and Rule 7.1.1 of the Local Rules of the United States District Court for the Southern District of New York, *Amicus* AT&T Corp., by its attorneys, Sidley Austin LLP, hereby provides the following disclosure:

AT&T Corp. is a wholly owned subsidiary of AT&T Inc., a publicly traded company. No entity owns more than 10% of AT&T Inc. stock.

Dated: June 11, 2014

Respectfully submitted,

/s/ Alan Charles Raul

Charles W. Douglas*
SIDLEY AUSTIN LLP
One South Dearborn
Chicago, Illinois 60603
(312) 853-7000
cdouglas@sidley.com
* *Of Counsel*
Attorneys for AT&T Corp.

Alan Charles Raul
Kwaku A. Akowuah
SIDLEY AUSTIN LLP
1501 K Street, NW
Washington, DC 20005
(202) 736-8000
araul@sidley.com
Attorneys for AT&T Corp.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION	13 Mag. 2814

Affidavit of Service

STATE OF NEW YORK)
ss:
COUNTY OF NEW YORK)

NICHOLAS J. LA FORGE, being duly sworn, deposes and says:

1. I am over eighteen (18) years of age, not party to this action, and am employed by the law firm of Sidley Austin LLP, located at 787 Seventh Avenue, New York, NY 10019.

2. On June 11, 2014, I served the following documents via U.S. Mail by enclosing a true and correct copy of same in a postage prepaid wrapper and depositing it in a depository maintained by the U.S. Postal Service at 787 Seventh Avenue, New York, NY 10019:

   a. Notice of Appearance of Alan Charles Raul, Esq., on behalf of *Amicus* AT&T

   b. *Amicus* AT&T's Rule 7.1 Disclosure

   c. Notice of Motion of AT&T Corp. for Leave to File a Brief as Amicus Curiae

d. Declaration of Alan Charles Raul in Support of Motion for Leave to File a Brief as Amicus Curiae with annexed Exhibit A

e. Memorandum of Law in Support of Motion of AT&T Corp. for Leave to File a Brief as *Amicus Curiae* in Support of Microsoft Corporation

3. Parties receiving service:

Guy Petrillo
Nelson A. Boxer
PETRILLO KLEIN & BOXER LLP
655 Third Avenue
New York, NY 10017

E. Joshua Rosenkranz
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Nancy Kestenbaum
Claire Catalano
COVINGTON & BURLING LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018

James M. Garland
Alexander A. Berengaut
COVINGTON & BURLING LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004

NICHOLAS J. LA FORGE

Sworn to before me this
11th day of June, 2014

Notary Public

RICARDO A. MURRAY
Notary Public, State of New York
No. 01MU4995024
Qualified in Kings County
Commission Expires April 13, 20

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

16 PŘÍLOHA Č. 5

16.1 ODKAZ

https://www.czso.cz/csu/czso/lidske_zdroje_v_informacni_spolecnosti_it_odbornici

16.1.1 OBSAH

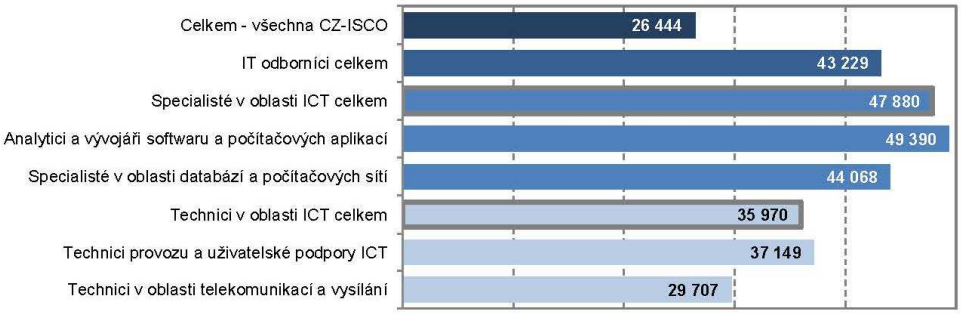
tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Mzdy IT odborníků v České republice

V roce 2013 se průměrný hrubý měsíční plat IT odborníka pohyboval nad hranicí 43 tisíc korun. A IT odborníci tak měli v průměru o téměř 17 tisíc korun vyšší mzdu, než jaký byl průměr za celou Českou republiku. O jedenáct let dříve, v roce 2002 činil průměrný měsíční plat IT odborníka 26,5 tisíc korun a byl o necelých 7 tisíc korun vyšší, než jaká byla průměrná mzda v ČR. Z uvedeného je patrné, že se během sledovaných let prohloubil rozdíl mezi mzdou IT odborníků a průměrnou mzdou za celou ČR.

Mezi jednotlivými **skupinami zaměstnání** jsou v platech IT odborníků poměrně velké rozdíly. Jak lze předpokládat, vyšší průměrnou hrubou měsíční mzdu mají Specialisté v oblasti informačních komunikačních technologií (dále jen ICT), kteří se zejména podílí na vývoji nových technologií a programování. Jejich mzda v roce 2013 činila bezmála 48 tisíc korun. Technici v oblasti ICT pak mají průměrnou měsíční mzdu o cca 12 tisíc korun nižší. Mezi Specialisty dosahují na vyšší mzdy Analytici a vývojáři softwaru, kteří berou v průměru 49 tisíc korun, kdežto Specialisté v oblasti databází cca 44 tisíc korun. Ve skupině techniků v oblasti ICT jsou na tom s platem výrazně lépe Technici provozu a uživatelské podpory ICT (37 tisíc korun) než Technici v oblasti telekomunikací a vysílání (30 tisíc korun).

Graf 1: Průměrná hrubá měsíční mzda v ČR* (v Kč), 2013

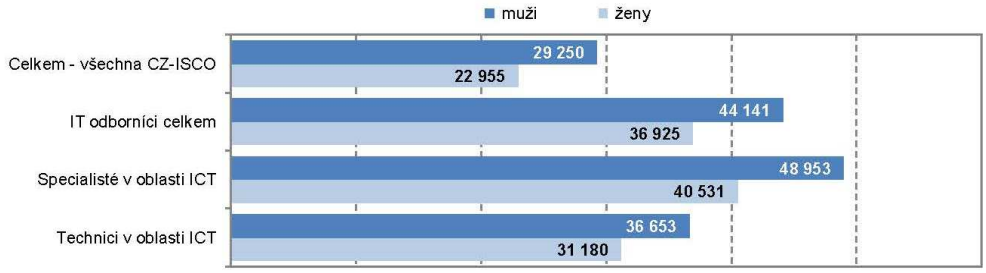


Zdroj: Strukturální mzdová statistika 2013

Průměrná hrubá měsíční mzda odborníků podle socio-demografických charakteristik

Ve výši průměrné hrubé měsíční mzdy IT odborníků existují mezi **muži a ženami** rozdíly, stejně jako je tomu i v případě celkových mezd v ČR. V roce 2013 dosáhl průměrný plat mužů na pozicích IT odborníků bezmála 44 tisíc korun a v případě žen činil necelých 37 tisíc. Průměrná mzda žen zaměstnaných na IT pozicích se tak pohybuje na 84 % mzdy mužů. V případě celkové hrubé měsíční mzdy v Česku je rozdíl mezi ženami a muži větší, v tomto případě činil průměrný plat žen 78 % průměrného platu mužů. Ve skupině zaměstnání Specialisté v oblasti ICT byl rozdíl mezi platy mužů a žen nepatrně větší než u IT odborníků celkem, ženy v této skupině zaměstnání dostávaly 83 % platu mužů. Naopak ženy zaměstnané jako Technici v oblasti ICT měly 85 % platu mužů zaměstnaných v této skupině zaměstnání.

Graf 2: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání a pohlaví (v Kč), 2013

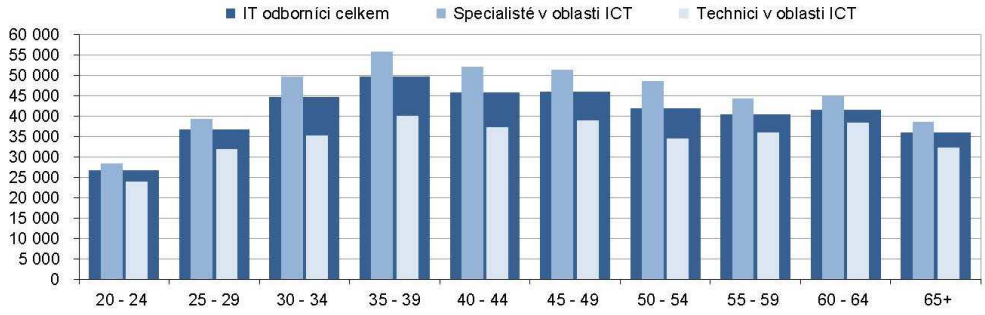


Zdroj: Strukturální mzdová statistika 2013

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Rozložení platů IT odborníků do jednotlivých **věkových skupin** kopíruje rozložení celkových platů v Česku. Tzn., že mzdy nerostou úměrně s věkem, ale svého maxima dosáhnou u osob z věkové skupiny 35 – 39 let a u vyšších věkových skupin již dochází k poklesu s mírným vzestupem od věku 55 let. Ten je pravděpodobně způsoben faktem, že zaměstnanci s vyšším platem zůstávají v zaměstnání déle. Obecně platí, že nejnižší platy mají zaměstnanci v nejnižších věkových skupinách, tzn. na počátku své kariéry a následně dochází k prudkému nárůstu platů s již zmíněným vrcholem ve věku 35–39 let. V této věkové skupině dosahuje průměrná hrubá měsíční mzda IT odborníka 49,6 tisíc korun, v případě Specialistů v oblasti ICT dokonce průměrná hrubá měsíční mzda v tomto věku blíží k hranici 56 tisíc korun, kdežto Technici v oblasti ICT v této věkové skupině pobírají téměř 40 tisíc korun. Ve všech věkových skupinách platí pravidlo, že lépe jsou v oblasti výpočetní techniky platově ohodnoceni Specialisté v ICT než Technici.

Graf 3: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání a věkových skupin (v Kč), 2013

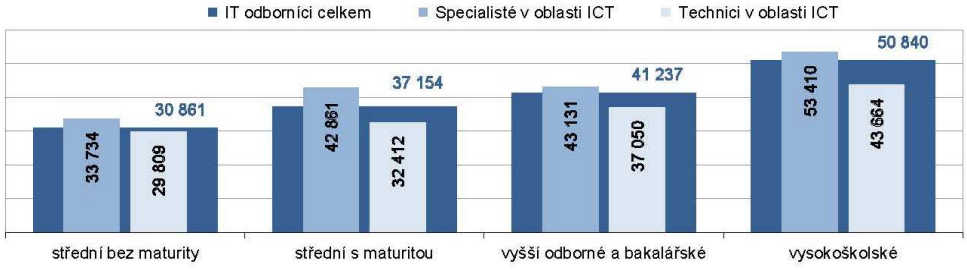


Zdroj: Strukturální mzdová statistika 2013

Nikoho asi nepřekvapí, že se vzrůstajícím **stupněm dosaženého vzdělání** IT odborníka narůstá i výše jeho platu. Toto pravidlo ostatně platí u všech zaměstnání a tak ani IT odborníci nejsou výjimkou. Průměrná mzda IT odborníka s vysokoškolským vzděláním byla v roce 2013 o více než 13 tisíc korun vyšší než IT odborníka se středním vzděláním s maturitou. Zatímco mezi IT odborníkem s maturitou a IT odborníkem s vyšším odborným či bakalářským vzděláním je ve výši platu rozdíl pouze 4 tisíce korun, pak mezi IT odborníkem s vyšším odborným či bakalářským vzděláním a IT odborníkem s vysokoškolským vzděláním je již rozdíl více než 9 tisíc korun.

Pokud se podíváme detailněji na dvě hlavní skupiny IT odborníků, je zřejmé, že v případě mezd Specialistů v ICT nezáleží na tom, zda mají vzdělání střední s maturitou nebo vyšší odborné či bakalářské, v obou případech totiž pobírají měsíčně cca 43 tisíc korun. Vysokoškolsky vzdělaní ICT specialisté však pobírají již 53 tisíc měsíčně. U Techniků v oblasti ICT jsou v jednotlivých vzdělanostních skupinách patrné větší rozdíly ve mzdách, kdy technici s maturitou měli v roce 2013 průměrnou mzdu 32 tisíc korun, technici se vzděláním vyšším odborným či bakalářským 37 tisíc a technici s vysokoškolským vzděláním pak měsíčně pobírali v průměru téměř 44 tisíc korun.

Graf 4: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání a nejvyššího dosaženého vzdělání (v Kč), 2013



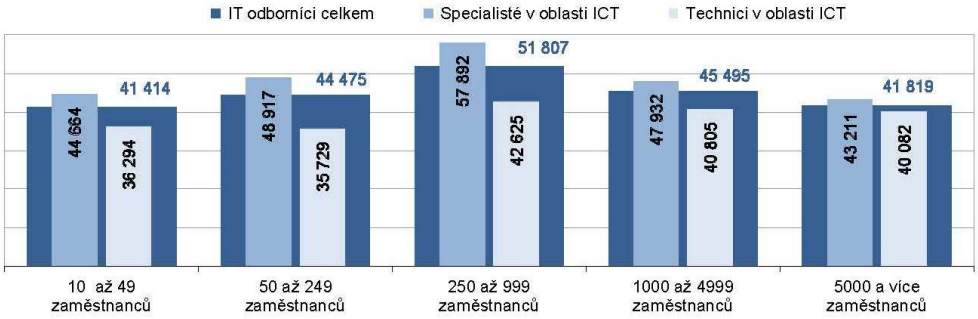
Zdroj: Strukturální mzdová statistika 2013

Průměrná hrubá měsíční mzda IT odborníků podle doby zaměstnání, velikosti podniku a sféry působení

Počet let strávených v jednom zaměstnání má samozřejmě vliv na růst mezd pracovníků, nejedná se však, na rozdíl od celkových mezd v ČR, o vztah přímo úměrný. V případě IT odborníků mají nejvyšší průměrnou hrubou měsíční mzdu zaměstnanci pracující u jednoho zaměstnavatele 13 až 14 let (47 tisíc korun) s tím, že již po 5 až 6 letech u jednoho zaměstnavatele překročí hranici 45 tisíc korun a dále dochází ve mzdách k výkyvům. Dokonce již po jednom roce u jednoho zaměstnavatele překročí průměrná měsíční mzda IT odborníka hranici 40 tisíc korun.

V případě celkových průměrných hrubých měsíčních mezd v Česku dochází se zvětšujícím se podnikem ke zvyšování průměrných mezd, kdežto u IT odborníků je situace poněkud odlišná. Průměrné platy u IT odborníků dosahují maximálních hodnot u podniků s 250 – 999 zaměstnanci (téměř 52 tisíc korun), v následující **velikostní kategorii** dochází k poklesu průměrného platu IT odborníků na 45 tisíc korun a ve skupině největších podniků se mzda ještě dále sníží na bezmála 42 tisíc korun. V případě obou hlavních skupin zaměstnání IT odborníků je trend rozložení platů malinko odlišný. Zatímco mzdy Specialistů kopírují mzdy IT odborníků jako celku, tzn nejvyšší mzdy pobírá tato skupina zaměstnaných v podnicích s 250–999 zaměstnanci (57,9 tisíc korun) a následuje relativně rychlý pokles výše mezd, tak mzdy Techniků v této velikostní skupině podniků přesáhnou hranici 42 tisíc korun a i ve větších podnicích pak zůstávají mzdy IT techniků nad hranicí 40 tisíc korun.

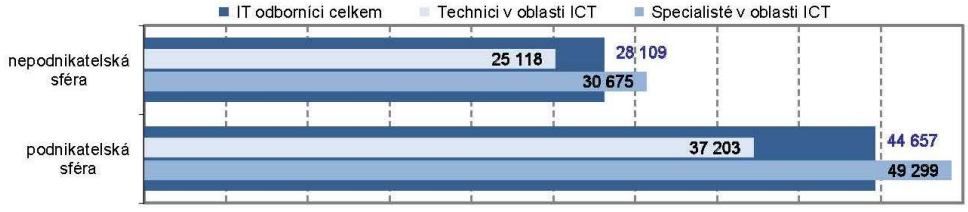
Graf 5: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání a velikosti podniku (v Kč), 2013



Zdroj: Strukturální mzdová statistika 2013

Významné rozdíly ve výši platů mezi IT odborníky jsou samozřejmě také podle toho, zda je daný odborník zaměstnán **v podnikatelské či nepodnikatelské sféře.** Nikoho asi nepřekvapí, že ve sféře podnikatelské jsou platy IT odborníků výrazně vyšší než v nepodnikatelské. Rozdíl průměrného platu IT odborníků zaměstnaných v těchto dvou rozdílných sférách činil v roce 2013 více jak 16 000 korun, což by se dalo popsat také tak, že IT odborník zaměstnaný v nepodnikatelské sféře pobíral pouhých 63 % platu IT odborníka zaměstnaného v podnikatelské sféře. Mezi dvěma hlavními skupinami zaměstnání IT odborníků jsou v průměrných platech podnikatelské sféry větší rozdíly než v případě sféry nepodnikatelské. V nepodnikatelské sféře činil v roce 2013 průměrný plat Technika v oblasti ICT 82 % platu Specialisty v oblasti ICT, kdežto ve sféře podnikatelské byl tento podíl 75 %.

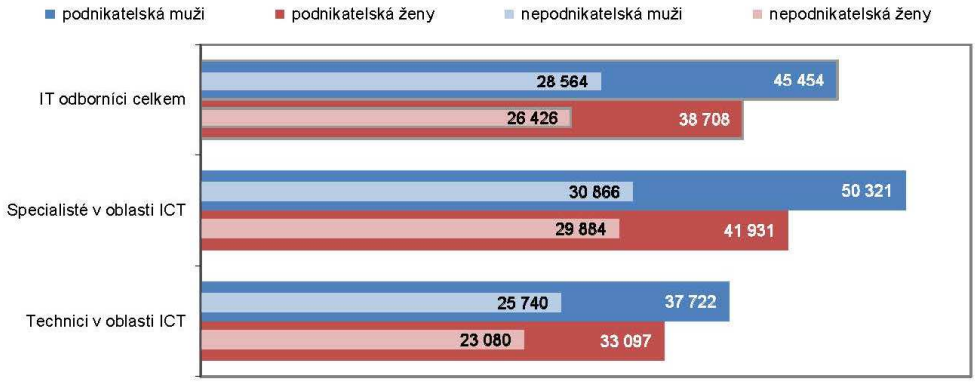
Graf 6: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání a sféry působení (v Kč), 2013



Zdroj: Strukturální mzdová statistika 2013

V případě dvou výše zmíněných sfér stojí za zmínku také rozdíly mezi průměrnými platy žen a mužů. V nepodnikatelské sféře pobírají ženy IT odbornice 93 % mzdy mužů IT odborníků, v podnikatelské sféře 85 %. Ve skupině Specialisté v oblasti ICT jsou v případě nepodnikatelské sféry platy ještě vyrovnanější, ženy dostávají 97 % průměrného platu mužů. Tyto rozdíly ve výši platů žen a mužů mezi zmiňovanými sférami jsou způsobeny tabulkovými platy v nepodnikatelské sféře, které neumožňují činit mezi muži a ženami výraznější rozdíly.

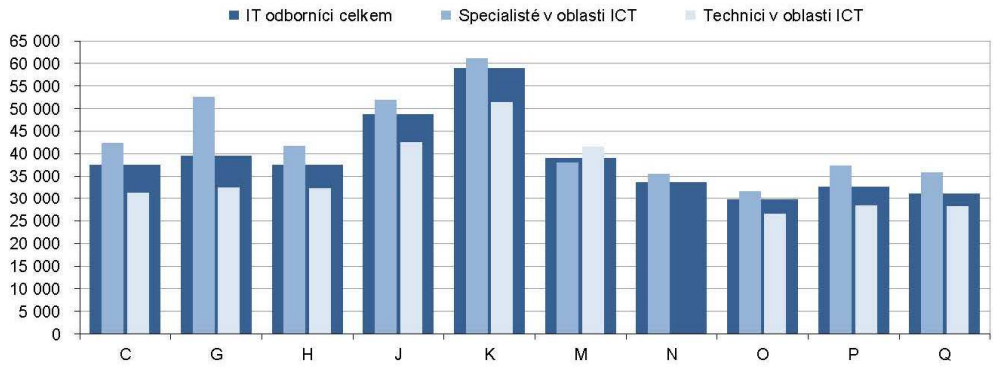
Graf 7: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání, sféry působení a pohlaví (v Kč), 2013



Zdroj: Strukturální mzdová statistika 2013

Tak jako existují rozdíly ve výši průměrných hrubých měsíčních mezd v rámci obou sledovaných skupin zaměstnání IT odborníků, tak také existují rozdíly ve výši mezd v rámci jednotlivých **odvětví (NACE)**. Nezanedbatelným faktem je tedy také, zda osoba zaměstnaná jako IT odborník pracuje v zemědělství, stavebnictví či v oblasti peněžnictví. Nejvyšších průměrných mezd dosahovali IT odborníci pracující v odvětví Peněžnictví a pojišťovnictví (58 900 korun) a nad ostatními odvětvími významně vyčnívají také Informační a komunikační činnosti, kde činil průměrný plat IT odborníka bezmála 49 tisíc korun. Naopak nejnižší mzdy pobírají IT odborníci zaměstnaní v odvětvích Zdravotní a sociální péče, Veřejná správa, obrana, sociální zabezpečení a Vzdělávání, kdy se pohybuje průměrná hrubá měsíční mzda IT odborníků těsně okolo třiceti tisíc korun.

Graf 8: Průměrná hrubá měsíční mzda IT odborníků podle zaměstnání a vybraných odvětví (v Kč), 2013



*Pozn: **C** - Zpracovatelský průmysl; **G** - Obchod; opravy motorových vozidel; **H** - Doprava a skladování; **J** - Informační a komunikační činnosti; **K** - Peněžnictví a pojišťovnictví; **M** - Profesní, vědecké a technické činnosti; **N** - Administrativní a podpůrné činnosti; **O** - Veřejná správa, obrana, sociální zabezpečení; **P** - Vzdělávání; **Q** - Zdravotní a sociální péče.*

Zdroj: Strukturální mzdová statistika 2013

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Průměrná hrubá měsíční mzda IT odborníků v krajích ČR

Významné jsou rozdíly v průměrných hrubých měsíčních platech IT odborníků mezi jednotlivými kraji České republiky. Není nikterak překvapivé, že nejvyšší hrubou průměrnou měsíční mzdu měli IT odborníci v hlavním městě Praze. Zde v roce 2013 dosahoval průměrný plat IT odborníka téměř 53 tisíc korun. Za Prahou druhý nejvyšší průměrný měsíční plat IT odborníka byl v roce 2013 v Jihomoravském kraji a dále v kraji Středočeském. Nejedná se však, o tak vysokou částku jako je tomu v případě hlavního města. Průměrná hrubá měsíční mzda IT odborníka byla v Jihomoravském kraji necelých 43 tisíc korun. V ostatních krajích se již průměrná mzda IT odborníků pohybuje v rozmezí 29–36 tisíc korun.

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

17 PŘÍLOHA Č. 6

17.1 ODKAZ

https://portal.mpsv.cz/sz/stat/vydelky/pra

17.1.1 OBSAH

nload/2014/pra_144_mzs.pdf

hlavní třída / třída zaměstnání CZ-ISCO		Hl. m. Praha	
		počet zaměstnanců přepočtený podle placených měsíců	hrubá měsíční mzda medián
		tis. osob	Kč/měs
D	Manuální pracovníci	167,6	19 278
T	Nemanuální pracovníci	380,0	32 824
1	Řídící pracovníci	35,2	57 745
11	Nejvyšší představitelé společností	2,7	66 577
12	Řídící prac.správy podniku, obchod., admin. a pod. činností	13,1	73 425
13	Řídící pracovníci výroby, IT, vzdělávání a příbuzných oborů	13,8	59 177
14	Řídící prac.ubyt.,strav.služeb,obchodu,ost.řídící pracovníci	5,7	31 494
2	Specialisté	124,5	40 745
21	Specialisté v oblasti vědy a techniky	29,2	38 446
22	Specialisté v oblasti zdravotnictví	5,1	35 321
23	Specialisté v oblasti výchovy a vzdělávání	11,3	32 846
24	Specialisté v obchodní sféře a veřejné správě	48,9	44 142
25	Specialisté v oblasti ICT	20,9	51 295
26	Specialisté obl. právní, sociální, kulturní a příbuz.oblastí	14,1	33 686
3	Techničtí a odborní pracovníci	131,9	31 425
31	Techničtí a odborní pracovníci v oblasti vědy a techniky	30,9	30 830
32	Odborní pracovníci v oblasti zdravotnictví	8,6	21 309
33	Odborní pracovníci v obchodní sféře a veřejné správě	77,1	32 491
34	Odborní pracovníci v obl.práva,kultury,sportu,příbuz.oborech	3,3	24 936
35	Technici v oblasti ICT	11,9	37 713
4	Úředníci	72,0	24 324
41	Všeobecní admin.pracovníci,sekretáři,pracovníci zadávání dat	26,1	24 750
42	Pracovníci informačních služeb,na přepážkách,v přib.oborech	21,0	23 613
43	Úředníci pro zpracování číselných údajů a v logistice	20,6	25 753
44	Ostatní úředníci	4,4	22 032
5	Pracovníci ve službách a prodeji	79,4	15 882
51	Pracovníci v oblasti osobních služeb	28,5	12 222
52	Pracovníci v oblasti prodeje	39,7	17 872
53	Pracovníci osob.péče ve vzdělávání,zdravotnictví,příbuz.obl.	1,4	19 794
54	Pracovníci v oblasti ochrany a ostrahy	9,8	12 219

load/2014/pra_144_pls.pdf

RSCP - platová sféra **rok 2014** **PLS-M7**

Hrubý měsíční plat podle hlavních tříd a tříd zaměstnání CZ-ISCO

hlavní třída / třída zaměstnání CZ-ISCO		Hl. m. Praha	
		počet zaměstnanců přepočtený podle placených měsíců	hrubý měsíční plat medián
		tis. osob	Kč/měs
D	Manuální pracovníci	14,0	18 048
T	Nemanuální pracovníci	109,1	30 454
1	Řídící pracovníci	7,2	47 219
11	Nejvyšší státní úřadníci, nejvyšší představitelé společností	1,6	52 837
12	Řídící prac.správy podniku, obchod., admin. a pod. činnosti	1,4	56 011
13	Řídící pracovníci výroby, IT, vzdělávání a příbuzných oborů	3,9	43 668
14	Řídící prac.ubyt.,strav.služeb,obchodu,ost.řídící pracovníci	0,2	40 366
2	Specialisté	41,2	31 055
21	Specialisté v oblasti vědy a techniky	3,2	34 121
22	Specialisté v oblasti zdravotnictví	8,5	38 342
23	Specialisté v oblasti výchovy a vzdělávání	13,9	27 070
24	Specialisté v obchodní sféře a veřejné správě	9,3	35 824
25	Specialisté v oblasti ICT	1,7	32 683
26	Specialisté obl. právní, sociální, kulturní a příbuz.oblasti	4,6	28 809
3	Techničtí a odborní pracovníci	42,9	29 952
31	Techničtí a odborní pracovníci v oblasti vědy a techniky	2,5	25 664
32	Odborní pracovníci v oblasti zdravotnictví	7,9	29 672
33	Odborní pracovníci v obchodní sféře a veřejné správě	29,5	30 906
34	Odborní pracovníci v obl.práva,kultury,sportu,příbuz.oborech	2,0	25 226
35	Technici v oblasti ICT	1,0	26 172
4	Úředníci	9,8	25 141
41	Všeobecní admin.pracovníci,sekretáři,pracovníci zadávání dat	3,4	25 411
42	Pracovníci informačních služeb,na přepážkách,v příb.oborech	0,5	22 694
43	Úředníci pro zpracování číselných údajů a v logistice	1,8	22 276
44	Ostatní úředníci	4,2	27 266

18 PŘÍLOHA Č. 7

18.1 ODKAZ

http://www.router-switch.com/Price-cisco-switches-cisco-switch-catalyst-2960_c19

18.2 OBSAH

- 1. **Products per page:**
  - 2. 25
  - 3. **50**
  - 4. 100
  - 5. 150

1. **Page:**
2. **1**
3. 2
4. Next >>

1.
2. **WS-C2960X-48TS-L**
   Conditions: Brand New Sealed
   Description: Catalyst 2960-X 48 GigE, 4 x 1G SFP, LAN Base
   Product Detail >>

   3. List Price:
   Our Price: **USD$1,510.00**

1.
2. **WS-C2960X-48TS-LL**
   Conditions: Brand New Sealed
   Description: Catalyst 2960-X 48 GigE, 2 x 1G SFP, LAN Lite
   Product Detail >>

   3. List Price:
   Our Price: **USD$1,247.00**

1.

2. **WS-C2960X-24PS-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 24 GigE PoE 370W, 4 x 1G SFP, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$1,346.00**

•

1.
2. **WS-C2960X-24PD-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 24 GigE PoE 370W, 2 x 10G SFP+, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$1,935.00**

•

1.
2. **WS-C2960X-24TD-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 24 GigE, 2 x 10G SFP+, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$1,639.00**

•

1.
2. **WS-C2960X-24TS-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 24 GigE, 4 x 1G SFP, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$879.00**

•

1.
2. **WS-C2960X-24TS-LL**

Conditions: Brand New Sealed
Description: Catalyst 2960-X 24 GigE, 2 x 1G SFP, LAN Lite
Product Detail >>

3. List Price:
Our Price: **USD$696.00**

•

1.
2. **WS-C2960X-48TD-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 48 GigE, 2 x 10G SFP+, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$2,326.00**

•

1.
2. **WS-C2960X-48LPS-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 48 GigE PoE 370W, 4 x 1G SFP, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$2,357.00**

•

1.
2. **WS-C2960X-48FPS-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 48 GigE PoE 740W, 4 x 1G SFP, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$2,778.00**

•

1.
2. **WS-C2960X-48LPD-L**
Conditions: Brand New Sealed

Description: Catalyst 2960-X 48 GigE PoE 370W, 2 x 10G SFP+ LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$3,022.00**

-

1.
2. **WS-C2960X-48FPD-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 48 GigE PoE 740W, 2 x 10G SFP+, LAN Base
Product Detail >>

3. List Price:
Our Price: **USD$3,454.00**

-

1.
2. **WS-C2960X-24PSQ-L**
Conditions: Brand New Sealed
Description: Catalyst 2960-X 24 GigE PoE, 2 x 1G SFP, 2 X 10/100/1000 BT, LAN Base
Product Detail >>

3. List Price:

Get a Quote

-

1. HOT

2. **WS-C2960S-48TS-L**
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-48TS Layer 2 - 48 x 10/100/1000 Ports - Gigabit Ethernet Switch - 4 x SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$1,695.00**

-

1. HOT

2. WS-C2960S-48TS-S
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-48TS Layer 2 - 48 x 10/100/1000 Ports - Gigabit Ethernet Switch - 2 x SFP - LAN Lite - Managed
Product Detail >>

3. List Price:
Our Price: **USD$1,452.00**

1. HOT

2. WS-C2960S-24TS-L
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-24TS Layer 2 - 24 x 10/100/1000 Ports - Gigabit Ethernet Switch - 4 x SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$1,110.00**

1. HOT

2. WS-C2960S-24TS-S
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-24TS Layer 2 - 24 x 10/100/1000 Ports - Gigabit Ethernet Switch - 2 x SFP - LAN Lite - Managed
Product Detail >>

3. List Price:
Our Price: **USD$901.00**

1. HOT

2. WS-C2960S-24PS-L
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-24PS Layer 2 - Gigabit Ethernet Switch - 24 x 10/100/1000 PoE Ports - 370W - 4 x SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$1,443.00**

- 1. HOT

2. WS-C2960S-48LPS-L
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-48LPS Layer 2 - Gigabit Ethernet Switch - 48 x 10/100/1000 PoE Ports - 370W - 4 x SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$2,260.00**

- 1. HOT

2. WS-C2960S-48FPS-L
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-48FPS Layer 2 - Gigabit Ethernet Switch - 48 x 10/100/1000 PoE Ports - 740W - 4 x SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$2,821.00**

-

1.
2. **WS-C2960S-24TD-L**
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-24TD Layer 2 - Gigabit Ethernet Switch - 24 x 10/100/1000 Ports - 2 x 10G SFP+ - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$1,668.00**

•

1.
2. **WS-C2960S-48TD-L**
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-48TD Layer 2 - Gigabit Ethernet Switch - 48 x 10/100/1000 Ports - Gigabit Ethernet Switch - 2 x 10G SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$2,327.00**

•

1.
2. **WS-C2960S-24PD-L**
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-24PD Layer 2 - Gigabit Ethernet Switch - 24 x 10/100/1000 PoE Ports - 370W - 2 x 10G SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$1,965.00**

•

1.
2. **WS-C2960S-48FPD-L**
Conditions: Brand New Sealed
Description: Cisco Catalyst 2960S-48FPD Layer 2 - Gigabit Ethernet Switch - 48 x 10/100/1000 PoE Ports - 740W - 2 x 10G SFP - LAN Base - Managed
Product Detail >>

3. List Price:
Our Price: **USD$3,419.00**

-

1.
2. **WS-C2960S-48LPD-L**
   Conditions: Brand New Sealed
   Description: Cisco Catalyst 2960S-48LPD Layer 2 - Gigabit Ethernet Switch - 48 x 10/100/1000 PoE Ports - 370W - 2 x 10G SFP - LAN Base - Managed
   Product Detail >>

3. List Price:
   Our Price: **USD$3,075.00**

-

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

19 PŘÍLOHA Č. 8

19.1 ODKAZ

http://www.globalpricelists.com/globalpricelistcisco.php

19.2 OBSAH

19.2.1 MODELOVÁ ŘADA

CISCO Global Price List

- Cisco 6015 IP DSL Switch
- Cisco 6160 IP DSL Switch
- Cisco 6260 IP DSL Switch
- Cisco 6400 Universal Access Concentrator
- Cisco 700 Series Products
- Cisco 7200 Series Products
- Cisco 7300 Series Products
- Cisco 7400 Series Products
- Cisco 7500 Series Products
- Cisco 7600 Series Router
- Cisco 7700 Series Products
- Cisco 800 Series Products
- Cisco 8100 Series Products
- CISCO AC/DC POWER SYSTEM
- Cisco Access Server 2500 Series Product
- Cisco Aironet
- Cisco AS5200 Series Products
- Cisco AS5300 Voice Gateway
- Cisco AS5350 Universal Gateway
- Cisco AS5400 Universal Gateway
- Cisco AS5400HPX Universal Gateway
- Cisco AS5800 Access Server
- Cisco AS5850 Universal Gateway
- Cisco ATA Series of Analog Telephone Adaptors
- Cisco BPX 8600 Series Products
- Cisco BTS 10200 Softswitch Series
- Cisco Building Broadband Products
- Cisco Carrier Routing System-1 Series
- Cisco Clean Access
- Cisco CVA120 Series Products
- Cisco DVB/DAVIC Series Products
- Cisco EGW 2200 Enterprise Gateway Product Family
- Cisco File Engine
- Cisco IAD2400 Integrated Access Devices
- Cisco IGX 8400 Series Products
- Cisco Information Center Products - CIC
- Cisco IP Telephony Solutions
- Cisco IP/TV
- Cisco IP/VC Videoconferencing Products
- Cisco MC3810 Series of Multiservice Access Routers
- Cisco MeetingPlace
- Cisco MGX 8230 & 8250 IP+ATM Edge Concentrators
- Cisco MGX 8260 Series Products
- Cisco MGX 8800 Series Products
- Cisco MGX 8880 Media Gateway
- Cisco MGX 8900 Series Products
- Cisco Mobile Wireless Edge Router Products
- Cisco PGW2200 Product Family
- Cisco Provisioning Center Products - CPC
- Cisco REGAN and RPM
- Cisco RF Switch Series Products
- Cisco SC2200 Product Family
- Cisco Service Control Products
- Cisco SIP Proxy Server
- Cisco SN 5400 Series
- Cisco SOHO Series

- Cisco Traffic Anomaly Guard & Detectors
- Cisco TransPath Series Products
- Cisco Transport Manager (CTM)
- Cisco uBR10012 Series Products
- Cisco uBR7100 Series Products
- Cisco uBR7200 Series Products
- Cisco uBR900 Series Products
- Cisco uMG9800 Series Products
- Cisco VCO/4K Series of Programmable Switches
- Cisco VPN 3000 Series Products
- Cisco WAN Management
- Cisco WT2700 Fixed Wireless Access
- CiscoSecure Access Control Server
- Configuration Services - TIS
- Consulting Services
- Contact Center Solutions
- Content Delivery Networks (Products)
- Data Center Software
- Documentation
- Implementation Offering -- TIS
- Installation Offering-TIS
- IPX Products
- Knowledge Transfer
- LightStream 1010 Products
- Mobile Routers
- Mobile Wireless Data Products
- Network Management
- Non-Contract Services
- onBusiness Network
- ONG AR1 Warranty Uplift - Annual (ON-AR1WTY-xxxx)
- ONG AR3 Warranty Uplift - Annual (ON-AR3WTY-xxxx)
- ONG OS1 Warranty Uplift - Annual (ON-OS1WTY-xxxx)
- ONG OS3 Warranty Uplift - Annual (ON-OS3WTY-xxxx)
- ONS 15104 Series Products
- ONS 15190 Series Products
- ONS 15216
- ONS 15302
- ONS 15305
- ONS 15327
- ONS 15454
- ONS 15454E
- ONS 15501
- ONS 15530
- ONS 15540 Series Products
- ONS 15600
- ONS 15800
- ONS 15801
- ONS 15808
- Peripheral Products Support - Software + 10 Day RTF (RR)
- Peripheral Products Support - Software + 8x5xNBD (NBD)
- Peripheral Products Support - Software Only (SW)
- PIX Firewall Series
- Redundant Power System & Misc Cables
- Security
- Service Expansion Shelf (SES) Products
- SMARTnet 24x7x2

- SMARTnet 24x7x4
- SMARTnet 8x5x4
- SMARTnet 8x5xNBD--
- SMARTnet Onsite 24x7x2
- SMARTnet Onsite 24x7x4
- SMARTnet Onsite 8x5x4
- SMARTnet Onsite 8x5xNBD
- Software Application Support
- Software Application Support Plus Upgrades
- SP Base + H/W 10 Day RTF - (SP-RR-xxx)
- SP Base + H/W Advance Replacement 24x7x2 - (SP-AR4-xxx)
- SP Base + H/W Advance Replacement 24x7x4 - (SP-AR3-xxx)
- SP Base + H/W Advance Replacement 8x5x4 - (SP-AR2-xxx)
- SP Base + H/W Advance Replacement 8x5xNBD - (SP-AR1-xxx)
- SP Base + H/W Onsite 24x7x2 - (SP-OS4-xxx)
- SP Base + H/W Onsite 24x7x4 - (SP-OS3-xxx)
- SP Base + H/W Onsite 8x5x4 - (SP-OS2-xxx)
- SP Base + H/W Onsite 8x5xNBD - (SP-OS1-xxx)
- SP Base Support - (SP-SW-xxx)
- SP Software Application Support + Upgrades - (SP-SAU-xxx)
- SP Software Application Support - (SP-SAS-xxx)
- Summa4 (VCO4K)
- Training
- Transceiver Modules
- Upgrade Offering-TIS
- Voice Network Switching Products (VNS)

19.2.2 CENÍK

Catalyst 3550 Series Workgroup Switches

Part Number	Product	GPL price in USD
WS-C3550-12G	10 GBIC ports + 2-10/100/1000 ports: EMI	9995 USD
WS-C3550-12T	10-10/100/1000 ports + 2 GBIC ports: EMI	9995 USD
WS-C3550-24-SMI	24-10/100 + 2 GBIC ports: SMI	2995 USD
WS-C3550-24-DC-SMI	24-10/100 + 2 GBIC ports(DC-Pwrd): SMI	4495 USD
WS-C3550-24-FX-SMI	24-100FX MMF + 2 GBIC ports: SMI	6495 USD
WS-C3550-24-EMI	24-10/100 + 2 GBIC ports: EMI	4990 USD
WS-C3550-48-SMI	48-10/100 + 2 GBIC ports: SMI	4995 USD

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

WS-C3550-48-EMI	48-10/100 + 2 GBIC ports: EMI	6990 USD
WS-C3550-24PWR-SMI	24-10/100 inline power + 2 GBIC ports: SMI	3495 USD
WS-C3550-24PWR-EMI	24-10/100 inline power + 2 GBIC ports: EMI	5490 USD

20 PŘÍLOHA Č. 9

20.1 ODKAZ

http://www.insight.com/en_US/buy/partner/fortinet.html?pq=%7B%22priceRangeLower%22%3A0%2C%22priceRangeUpper%22%3A0%2C%22sortBy%22%3A%22BestMatch%22%2C%22searchTerms%22%3A%7B%22FORTINET%22%3A%7B%22field%22%3A%22field%22%2C%22value%22%3A%22A-MARA-MFRNR~0007042037%22%7D%7D%7D

20.2 OBSAH

Fortinet FortiCare 24X7 Comprehensive Support - extended service agreement (renewal) - 1 year - shipment

Mfr Part #: FC110LV0VM-248-02-12 | Insight Part #: FC110LV0VM24802121

Add to My Compare List

Compare Similar

Show Details

USD $815.99

as low as $42.18/mo.

Unlimited availability

3YR 24X7 UTM BNDL FOR SVCSFORTIGATE-1000D

Mfr Part #: FC10-01006-950-02-24 | Insight Part #: FC100100695002241

Add to My Compare List

Compare Similar

Show Details

USD $18,840.99

as low as $973.89/mo.

Unlimited availability

Fortinet FortiCare 8x5 Enhanced Support - extended service agreement (renewal) - 1 year - shipment

Mfr Part #: FC-10-P0226-311-02-12 | Insight Part #: FC10P02263110212

Add to My Compare List

Compare Similar

Show Details

USD $94.99

as low as $4.91/mo.

Unlimited availability

Fortinet FortiGate 1000D - Bundle - security appliance

Mfr Part #: FG-1000D-BDL-950-36 | Insight Part #: FG1000DBDL95036

Add to My Compare List

Compare Similar

21 PŘÍLOHA Č. 10

21.1 ODKAZY

- http://www.dell.com/uk/business/p/storage-sc2000/fs
- http://www8.hp.com/cz/cs/products/disk-storage/product-detail.html?oid=5386548#!tab=specs

21.2 OBSAH

- Offer Price £17,189

Ex. VAT & Shipping

Delivery methods and timing may vary, click for more information.

Now Accepting PayPal.

Will be dispatched in 5 - 7 working days

E-Value Code: DSSCV2000

- Offer Price £18,037

Ex. VAT & Shipping

Delivery methods and timing may vary, click for more information.

Now Accepting PayPal.

Will be dispatched in 5 - 7 working days

E-Value Code: DSSCV2020

- Offer Price £43,621

Ex. VAT & Shipping

Delivery methods and timing may vary, click for more information.

Now Accepting PayPal.

Will be dispatched in 8 - 10 working days

E-Value Code: DSSCV2080

- Offer Price £7,657

Ex. VAT & Shipping

Delivery methods and timing may vary, click for more information.

Now Accepting PayPal.

Will be dispatched in 5 - 7 working days

E-Value Code:DSSC100ENCLOSURE

- Offer Price £8,703

Ex. VAT & Shipping

Delivery methods and timing may vary, click for more information.

Now Accepting PayPal.

Will be dispatched in 5 - 7 working days

E-Value Code: DSSC120E

HP MSA 2040 SAS DC w/ 4x200GB SFF SSD 6x900GB 10K SFF HDD 1 Performance Auto Tier LTU 6.2TB Bundle(M0T61A)	HP MSA 2040 SAN DC w/ 4x200GB SFF SSD 6x900GB 10K SFF HDD 1 Performance Auto Tier LTU 6.2TB Bundle(M0T60A)	HP MSA 1040 1Gb iSCSI w/4 600GB SAS SFF HDD Bundle/TVlite(M0T22A)	HP MSA 2040 12Gb SAS w/6 600GB SAS SFF HDD Bundle/TVlite(M0T27A)
*Cena**	*Cena**	*Cena**	*Cena**
891 448 Kčs DPH	**894 857 Kč**s DPH	**138 527 Kč**s DPH	**211 363 Kč**s DPH
736 734 Kčbez DPH	**739 551 Kč**bez DPH	**114 485 Kč**bez DPH	**174 680 Kč**bez DPH

22 PŘÍLOHA Č. 11

22.1 ODKAZ

http://www.etb-tech.com/servers/dell-blade-servers/poweredge-m600

22.2 OBSAH

- **Dell Poweredge M600 Build To Order**

  From £125.00

  Price exc. VAT

  Configure your own server from a wide selection of components.

  1 Year ETB-TECH Warranty

  ETB-TECH Refurbished

Dell PowerEdge M600 Blade Server

£105.00

Price exc. VAT

- 2 x E5430 Xeon Quad-Core CPU
- 2.66GHz Processor Speed
- 8GB RAM
- 1 x 73GB 15K SAS Hard Drive
- SAS6/iR RAID
- Up to 2 x 2.5" HDDs

1 Year ETB-TECH Warranty

ETB-TECH Refurbished

-

PowerEdge M1000e Blade Enclosure with 16 x M600 Blades

£2,280.00

Price exc. VAT

- Each blade configured as below
- 2 x E5430 Xeon Quad-Core CPU
- 2.66GHz Processor Speed
- 8GB RAM
- 1 x 73GB 15K SAS Hard Drive
- SAS6/iR RAID

1 Year ETB-TECH Warranty

ETB-TECH Refurbished

- ## PowerEdge M1000e Blade Enclosure with 16 x M600 Blades

£2,400.00

Price exc. VAT

- Each blade configured as below
- 2 x E5450 Xeon Quad-Core CPU
- 3.0GHz Processor Speed
- 8GB RAM
- 1 x 73GB 15K SAS Hard Drive
- SAS6/iR RAID

1 Year ETB-TECH Warranty

ETB-TECH Refurbished

tel.: +420 257 289 112
fax: +420 257 289 212
e-mail: mail@relsie.cz

Dell PowerEdge M600 Blade Server

£85.00

Price exc. VAT

- 2 x E5405 Xeon Quad-Core CPU
- 2.0GHz Processor Speed
- 4GB RAM
- 0 x 2.5" Hard Drives
- SAS6/iR RAID
- Up to 2 x 2.5" HDDs