Příloha č. 4 – Technická specifikace

Požadavek na funkcionalitu

Požadujeme řešení postavené na licencování kapacit, zadavatel požaduje pokrýt min. 48TB primárních dat a min. 100 ks koncových zařízení (tj. dalších min. 2TB dat na PC nebo notebooku s OS Windows, Linux nebo MAC OS). Požadujeme, aby nabízené řešení podporovalo mobilní zařízení s OS Android a Apple IOS.

Popis rozdělení primárních dat:

Systém	**Typ dat**	**Počet ESX/počet VM/počet socketů**	**Celková velikost zálohovaných dat v GB**
Virtualizace	filesystemy VM	27/240/50	14000
Virtualizace	aplikace a DB VM		16000
Fyzické servery	filesystemy		5000
Fyzické servery	aplikace a DB		2000
CIFS/NFS shares	filesystemy		11000

Řešení musí umožnit uložit data v lokalitě zadavatele s retencí minimálně 1 rok, a současně archivní data až 5 let. Kritická data pak požadujeme zálohovat/replikovat do datacentra účastníka s vysokou úrovní dostupnosti a zabezpečení. Retence dat v datacentru je minimálně 1 měsíc. Data s retencí do jednoho měsíce musí být v lokalitě zadavatele držena v diskové záloze i na pásce, data o retenci vyšší než jeden měsíc mohou být v diskové záloze, ale musí být na pásce. Předpokládaný objem dat na páskách je ročně kolem 480 TB komprimovaně – kompresní poměr cca 1:2.

Dodané řešení musí umožnit vysokou dostupnost a zálohování i obnova musí být funkční i v případě výpadku komunikace mezi lokalitou zadavatele a lokalitou dodavatele. Požadujeme funkci automatického pokračování zálohování i replikací po obnovení spojení.

Dodané řešení musí umožnit navýšit licenční kapacitu zálohování zdrojových dat kdykoliv během platnosti služby. Kapacita musí jít navýšit s rozlišením 1 TB. Dodavatel musí být schopen navýšit kapacitu poskytovaných či klientských licencí zálohování až o 100 %, a to nejpozději do 3 dnů od zadání požadavku zadavatele.

Řešení musí umožnit zálohování a obnovu dat dle specifikace a zároveň musí podporovat archivaci pro souborové systémy a virtuální stroje. Stejně tak požadujeme zálohování i archivaci produktu MS Exchange Cluster DAG 2016 o předpokládané kapacitě až 25 TB dat s možností růstu až na 4000 mailboxů. V úvodní konfiguraci požadujeme pokrytí licencí pro zálohu MS Exchange 2016 o kapacitě 10 TB/4000 mailboxů s možností granulární obnovy na úrovni jednotlivé zprávy z celé zálohy.

V úvodní konfiguraci požadujeme pokrytí archivační licence na minimálně 50 mailboxů s možností rozšíření a dokupu licencí až na 4000 mailboxů. Archivací zde nerozumíme uložení zálohy po delší retenční dobu, ale aktivní přesun dat na jiné úložiště tak, aby se data nemusela znovu zálohovat a ani obnovovat, tedy aby bylo dosaženo snížení RTO a RPO. Předpokládáme pokročilé techniky archivní služby jako je vyhledávání v archivu, deduplikace archivního úložiště, indexace, možnosti převodu uživatelských PST složek do archivu, dostupnost archivu pro uživatele i v případě nedostupnosti MS Exchange serveru. Stejně tak požadujeme podporu archivace produktu MS Exchange 2016 a podporu archivace exportovaných dat z aplikace Groupwise 2014.

Řešení musí umožnit migraci a obnovu již zazálohovaných fyzických serverů do virtuálního prostředí Vmware.
Řešení musí umožnit provedení Disaster Recovery fyzických i virtuálních serverů. Pro virtuální servery běžící v prostředí Vmware, požadujeme funkcionalitu Instant Recovery – možnost startovat virtuální server přímo z backupu.
Požadujeme zálohu provozovaného virtuálního prostředí Vmware a na úrovni image zálohy.
Požadujeme integraci zálohovacího řešení pro zálohování snapshotů a clonů na diskovém poli HP 3PAR a IBM Storwize v7000, včetně vytváření a práce s daty uvnitř těchto snapshotů pomocí zálohovacího prostředí (například data ze snapshotů budou využita pro zálohy, ale i obnovu pro kritické RTO a RPO) ve spolupráci s virtualizovaným prostředím Vmware.
Vyžadujeme zajištění aplikační konzistence pro Oracle, MS SQL, VMware, MS Exchange 2016 a souborové systémy Windows a Linux, GroupWise 2014.
Maximální doba zálohy pro 1 TB zdrojových dat bude 1 hodina (při maximální paralelizaci 1).
Maximální doba obnovy pro 1 TB zdrojových dat bude 1 hodina (při maximální paralelizaci 1).
Požadujeme centrální (globální) deduplikaci s podporou deduplikace na klientech zálohovacího prostředí. Deduplikace bude dostupná pro všechny zmíněné funkce a bude deduplikovat všechna data napříč celým řešením a dostupnou funkcionalitou. Požadována je i deduplikace na pásky LTO.
Požadujeme jednotný management (jednotnou konzoli) pro správu a konfiguraci celého prostředí (zálohování, archivace, replikace, řízení snapshotů diskových polí, správa účtů, granulární obnova).
Replikace dat (mezi všemi lokalitami - primární a záložní (cloud lokalitou) lokalitou musí probíhat v deduplikované podobě – replikují se pouze změněné bloky dat.
Požadujeme podporu souborových systémů Windows, Linux (SuSe, Oracle, RedHat, Novell OES, Debian, Windows 2008,2012,2016,7,8,8.1,10 a MacOS).
Požadujeme nativní podporu CDP/CDR (Continuous Data Protection a Continuous Data Replication) pro data uložena na fibre-channel diskových oblastech libovolných výrobců diskového pole a to primárně pro Oracle databázi a GroupWise 2014 data. Možnost okamžité replikace uložených kritických dat.
V současné době využíváme zálohovací prostředí CommVault. Požadujeme u platných záloh s retencí delší než jeden měsíc provedení převodu/migrace zazálohovaných dat do nabízeného řešení z důvodu zajištění kontinuity zálohovaných dat Předpokládaná kapacita dat pro migraci je cca 300 TB dat komprimovaných dat, tj. 600 TB dat nekomprimovaných). Data jsou uložena na páskách LTO6/7 a v deduplikačním disku spravovaném aplikací Commvault. Správnost migrace požadujeme otestovat zkušením restorem Vmware image, Oracle DB a granulární obnovou souboru z Vmware Image.
V případě dodávaného řešení požadujeme potvrzení kompatibility dodávaného řešení jednak dodavatelem řešení, tak i výrobcem podporovaných technologií. Jedná se hlavně o prostředí integrace Vmware, XEN, OpenStack, Oracle RAC, HP 3PAR, IBM Storwize v7000, Novell, MS Exchange 2016 archivace i cloud služeb.

GPDR – požadujeme vyjádření výrobce či dodavatele jak splňuje a řeší legislativu Evropské unie - General Data Protection Regulation. V podrobné technické specifikaci účastník uvede alespoň URL odkaz na vyjádření výrobce technologie k problematice splnění požadavků GDPR.
Řešení musí umožnit uložit data v lokalitě zadavatele s retencí minimálně 1 měsíc a současně vybraná kritická data replikovat do geograficky vzdáleného datacentra (záložní lokalita) účastníka s vysokou úrovní dostupnosti. Replikace dat je požadována přes zabezpečenou VPN linku.
Řešení musí umožnit navýšení kapacitu zálohování zdrojových dat kdykoliv během platnosti služby. Účastník musí být schopen navýšit kapacitu v datovém centru i poskytované licence zálohování až o 50 %, a to nejpozději do 4 hodin od zadání požadavku.
Řešení musí umožnit migraci zálohovaných fyzických serverů do virtuálního prostředí Vmware. Stejně tak řešení musí umožnit provádění Disaster Recovery fyzických i virtuálních serverů.
Požadujeme podporu zálohování snapshotů a clonů na diskovém poli HP 3PAR, HP P6000 a IBM Storwize v7000, včetně vytváření a práce s daty uvnitř těchto snapshotů pomocí zálohovacího prostředí (například data ze snapshotů budou využita pro zálohy, ale i obnovu pro kritické RTO a RPO). Vyžadujeme zajištění aplikační konzistence pro Oracle, MS SQL, VMware , MS Exchange 2016 a souborové systémy Windows a Linux a Novell.
Požadujeme centrální (globální) deduplikaci s podporou deduplikace na klientech zálohovacího prostředí. Deduplikace bude dostupná pro všechny zmíněné funkce a bude deduplikovat všechna data napříč celým řešením a dostupnou funkcionalitou.
Replikace dat mezi primární a záložní lokalitou v deduplikované podobě – replikují se pouze změněné bloky dat.
Podpora efektivního zálohování poboček nebo vzdálených zařízení. Požadovaná je již zmíněná replikace deduplikovaných dat do datacentra (záložní lokality) a podpora obnovy dat včetně „bare-metal-recovery“ obnovy v záložní lokalitě.
Monitoring: Zadavatel požaduje přístup a možnost kontrolovat prostředí zálohování. Požadujeme auditování přístupů do zálohovacího prostředí a vytvoření definovaných přístupů zaměstnanců zadavatele s možností provádět obnovy i zálohy celého prostředí. Vzhledem k rozsahu prostředí požadujeme definici přístupů tak, aby konkrétní administrátor zadavatele mohl pouze zálohovat, měnit či vytvářet zálohy a obnovovat data a systémy, které spravuje a to i na úrovni databází, aplikací i OS.
Požadujeme automatické vytváření denního a měsíčních reportu o stavu zálohování a o všech provedených změnách účastníkem. Požadujeme podporu ukládání dat na magnetické pásky. Požadujeme provádění správy médií a tvorbu reportů pro data uložena na páskách a odesílána pro kontrolu zadavateli (operace musí být maximálně automatizované – například řešení bude generovat čísla pásek a informace o zálohovaných datech, aby byl snadný export a import).
Telefonická podpora 24x7 v českém jazyce, jednotné kontaktní místo pro hlášení problémů v době od 8:00 do 16:30. U kritického incidentu zahájit řešení do 4 hodin. U urgentního incidentu zahájit řešení do 8 hodin. U méně závažného incidentu zahájit řešen do 72 hodin Obnova kritických serverů do 24 hodin. Konzultace a poradenství v rozsahu minimálně 1 MD měsíčně v ceně plnění,

Poskytnutí součinnosti při řešení změn na straně zadavatele, zejména při zapracování změn architektury informačních systémů zadavatele.

Dostupnost služby min. 99 %.

Definice typů incidentů dle jejich závažnosti:

1. **Kritický incident**

   Kritickým incidentem se rozumí stav celkové nefunkčnosti nebo nemožnosti využívání klíčových funkcionalit zařízení nebo systému. Uživatelé systému nemohou v takovém případě využívat služeb, které má systém poskytovat. Typicky se jedná o nefunkční zálohování kritických dat, nefunkční obnova souborů nebo emailových zpráv apod.

2. **Urgentní incident**

   Urgentním incidentem se rozumí takový stav zařízení či systému, kdy je některá komponenta nebo součást systému mimo provoz či neplní svoji funkci, ale systém jako celek je stále schopen alespoň omezeně poskytovat své služby či plnit svou funkcionalitu. Uživatelé mohou v takovém případě stále využívat služeb systému. Příkladem vážné poruchy bývá zpravidla výpadek některé redundantní komponenty zařízení (např. disk, řadič, zdroj, apod.) nebo celého zařízení, které tvoří součást clustrového řešení.

3. **Méně závažný incident**

   Méně závažným incidentem se rozumí takový stav zařízení nebo systému, který neodpovídá předávací dokumentaci, ale neohrožuje klíčové funkcionality řešení.

Data musí být umístěna na území EU

Data umístěna minimálně ve 2 kopiích na fyzicky odděleném hardware v synchronní replikaci v rámci minimálně jednoho datového centra.

Zadavatel požaduje přístup 24/7 do management konzole ke zdrojům umístěným v datovém centru.

Zadavatel požaduje mít přes management konzoli možnost navýšit vysoutěženou kapacitu infrastruktury v datovém centru o min. 50% původní kapacity. Zároveň požaduje, aby navýšenou kapacitu měl k dispozici nejpozději do 4 hodin od zadání požadavku na navýšení kapacity. Kapacitu nad rámec poptávané kapacity Zadavatel požaduje platit na měsíční bázi podle skutečně TB.

Zadavatel požaduje nativní integraci mezi zálohovacím software a poptávaném prostředí v datovém centru (místo pro ukládání záloh v datovém centru lze namapovat a připojit přímo z administrační konzole zálohovacího software). Nativní podpora znamená spolupráci a integraci s API vrstvou prostředí mezi zálohovacím prostředím a cloud prostředím.

Zadavatel požaduje možnost vytvoření výpočetních zdrojů ze strany zadavatele v prostředí datového centra bez nutnosti asistence účastníka služby pro případ Disaster Recovery.

Zadavatel požaduje nativní integrace zálohovacího řešení s prostředím v datovém centru pro případ Disaster Recovery.

Zadavatel požaduje účtování výpočetních zdrojů v cloud prostředí pro případ Disaster Recovery na hodinové bázi.

Zadavatel poptává min. 60 TB čisté kapacity v datovém centru

Podrobný popis požadovaných služeb zálohování a archivace provozované v režimu BaaS – Backup as a Service

V rámci požadavků zálohovaní a archivace rozsáhlého prostředí informačních systémů zadavatele je požadována služba zálohování a archivace tomto rozsahu a dle této specifikace:

1/ Popis prostředí

Zadavatel využívá ve svém centrálním zálohovacím systému řešení Commvault Data Protection verze 11 v konfiguraci se zálohováním do minimálně dvou nezávislých lokálních diskových úložišť, na lokální páskovou knihovnu typ MSL6480 s 2xLTO7 FC mechanikou a 80 sloty a zálohováním/replikací do cloud prostředí v geograficky oddělené lokalitě. Páskovou knihovnu MSL6480 chce zadavatel nadále využívat pro ukládání dat jako sekundární úložiště s dlouhodobou retencí, viz popis níže. Navrhovaném řešení musí dále zajistit i potřebnou kapacitu pro dlouhodobou archivaci dat (magnetická media LTO6/LTO7). Dodávka pásek LTO6/LTO7 není předmětem této veřejné zakázky.

Prostředí zadavatele zahrnuje více než 30 fyzických serverů, 27 virtualizačních hypervisorů se 180 provozovanými virtuálními servery a stovky koncových zařízení typu desktop, notebook nebo tablet. Data jsou uložena na discích fyzických serverů a na diskových úložištích HP 3PAR, IBM Storwize 7000 a Bosson, u virtualizačních hypervisorů jsou data uložena výhradně na uvedených diskových úložištích (dále jen primární data). Tato disková úložiště jsou lokalizována v areálu zadavatele (hlavní lokalita) ve dvou technických místnostech, které jsou propojené síťovými technologiemi SAN 8Gb/s a LAN 10Gb. Většina zálohovaných systémů je rovněž kompatibilní s těmito síťovými technologiemi.

Kromě hlavní lokality zadavatele existuje také vzdálená lokalita, ve které se provozují 2 virtualizační hypervisory o celkové kapacitě produkčních dat 1,5 TB. Tento objem dat je zahrnut do poptávané kapacity. Propustnost datové linky ze vzdálené lokality do Internetu je 150 Mb/s a požadavek na datové RTO (Recovery Time Objective) je max. 24 hodin.

Vzhledem k očekávanému nárůstu objemu dat z IS, možným změnám počtů jednotlivých prvků v zálohovacím prostředí a jednoduchosti správy celého zálohovacího a archivačního prostředí požadujeme návrh v modelu kapacitních licencí pro software komponenty.

Zadavatel požaduje kompletní dodávku HW i SW vybavení pro celé zálohovací prostředí v rámci služby BaaS. Požadované schéma ochrany dat předpokládá 3 typy úložišť:

a) zálohování do centrálního úložiště či výpočetního systému s diskovým úložištěm (zajišťuje dodavatel BaaS), umístěno v hlavní lokalitě
b) archivace do páskové knihovny MSL6480, umístěna v hlavní lokalitě
c) replikace do cloud úložiště dodavatele (zajišťuje dodavatel BaaS). Kapacita úložiště musí být dimenzována s dostatečnou kapacitou držení (retence) dat v diskovém úložišti po dobu min. 30 dní (cca 4 x Full Backup a 22 x Increment. Backup), tj. 48 TB zdrojových nededuplikovaných dat.

Licenčně je tedy potřeba pokrýt minimálně 48 TB primárních dat a 100 ks koncových zařízení (cca dalších až 1 TB dat/PC, notebook, tablet s OS Windows, Linux a MAC). Požadujeme podporu mobilních zařízení Android a Apple IOS.

2/ Struktura zálohovaných a archivovaných dat

2.1 Struktura primárních dat:

Systém	**Typ dat**	**Počet ESX/počet VM/počet socketů**	**Celková velikost zálohovaných dat v GB**
Virtualizace	filesystemy VM	27/240/50	14000
Virtualizace	aplikace a DB VM		16000
Fyzické servery	filesystemy		5000
Fyzické servery	aplikace a DB		2000
CIFS/NFS shares	filesystemy		11000

Navržené řešení musí umožnit uložit primární data v hlavní lokalitě zadavatele s požadovanou retencí a současně archivní data na požadovanou dobu. Kritická primární data pak požadujeme zálohovat/replikovat do cloud úložiště dodavatele s vysokou úrovní dostupnosti a zabezpečení. Požadovaná retence dat v cloud úložišti je uvedena v technické specifikaci. Primární data s retencí menší nebo rovnou 1 měsíci musí být v primární lokalitě zadavatele držena v centrálním úložišti (úložiště typu a)) i na páskové knihovně (úložiště typu b)), primární data o retenci vyšší než jeden měsíc mohou být v centrálním úložišti, ale vždy **musí** být na páskové knihovně. Předpokládaný objem dat na mediích LTO 6/7 je ročne min. 500 TB.

2.2 MS Exchange data

Zadavatel požaduje plnou podporu zálohování i archivace produktu MS Exchange 2016. V úvodní konfiguraci zadavatel požaduje pokrytí sw licencí pro **zálohu** MS Exchange 2016 o kapacitě 10 TB/3000 mailboxů s možností **granulární** obnovy na úrovni jednotlivé zprávy z celé zálohy.

Zadavatel v úvodní konfiguraci požaduje pokrytí **archivační** licence na minimálně 50 mailboxů s možností rozšíření a dokupu licencí až na 4000 mailboxů.

Zadavatel požaduje plnou podporu archivace prostředí Groupwise 2014.

3/ Požadavky na umístění dat a integraci přístupu ke zdrojům umístěným v cloud úložišti:

- Cloud úložiště je poskytováno z datového centra na území EU a zálohovaná data musí být umístěna na území EU.
- Redundance minimálně na úrovni N+1 (napájení a chlazení).
- Víceúrovňová ochrana datového centra, ve kterém je provozována služba cloud úložiště.
- 24/7 fyzická přítomnost bezpečnostní služby v datovém centru.
- Nepřetržitý kamerový dohled v datovém centru.
- Data umístěna minimálně ve 2 kopiích na fyzicky odděleném hardware v synchronní replikaci v rámci minimálně jednoho datového centra.
- Zadavatel požaduje přístup 24/7 do management konzole ke zdrojům umístěným v datovém centru.

- Zadavatel požaduje mít přes management konzoli možnost navýšit zasmluvněnou kapacitu infrastruktury v datovém centru min. o 50 %. Zároveň požaduje, aby navýšenou kapacitu měl k dispozici nejpozději do 4 hodin od zadání požadavku do management konzole. Tato navýšená kapacita bude fakturována jako speciální položka na měsíční bázi podle skutečně alokovaných zdrojů s rozlišením na 1 TB.
- Účastník musí garantovat nabídnutou cenu za navýšení kapacity po celé období platnosti smlouvy.
- Zadavatel požaduje nativní integraci mezi zálohovacím software a cloud úložištěm v datovém centru (tzn. místo pro ukládání záloh v datovém centru lze namapovat a připojit přímo z administrační konzole zálohovacího software). Nativní podpora také znamená spolupráci a integraci s API vrstvou prostředí zálohovacího software a cloud úložiště.
- Zadavatel požaduje mít možnost, aby mohl sám vytvářet výpočetní zdroje bez nutné asistence účastníka pro případ Disaster Recovery postupů.
- Zadavatel požaduje nativní integraci zálohovacího řešení s prostředím v datovém centru pro případ Disaster Recovery.
- Zadavatel požaduje účtování výpočetních zdrojů pro případ Disaster Recovery na hodinové bázi.
- Dodané řešení musí garantovat vysokou dostupnost a zálohování i obnova dat musí být funkční i v případě výpadku komunikace mezi primární lokalitou zadavatele a lokalitou účastníka. Požadujeme funkci automatického pokračování zálohování i replikací po obnovení spojení.

4/ Další obecné a implementační požadavky pro služby BaaS

4.1 Upřesnění pojmů Archivace a Replikace

Archivací se pro účel této veřejné zakázky **nerozumí** uložení zálohy po delší retenční dobu, ale **aktivní** přesun dat na jiné datové úložiště (typu a, b nebo c)tak, aby se data nemusela v mezikroku zálohovat a ani obnovovat, tedy bylo dosaženo snížení RTO a RPO (Recovery Point Objective).

Replikace dat (mezi hlavní lokalitou, vzdálenou lokalitou a data centrem, odkud je poskytována služba cloud úložiště) probíhá v deduplikované podobě a replikují se pouze změněné bloky dat.

4.2 Implementační požadavky:

- možnost využití pokročilých technik archivní služby jako je vyhledávání v archivu, deduplikace archivního úložiště, indexace, zpřístupnění možnosti převodu uživatelských PST složek do archivu atd.;
- umožnit migraci a obnovu již zazálohovaných fyzických serverů do virtuálního prostředí VMware;
- umožnit provedení Disaster Recovery fyzických i virtuálních serverů. Pro virtuální servery běžící v prostředí VMware, je požadována funkcionalita Instant Recovery, tj. možnost startovat virtuální server přímo ze záložní kopie;
- granulární obnovu souborů ze všech požadovaných OS, viz níže Podporu souborových systémů Windows, Linux (SuSe, Oracle, RedHat, Novell OES, Debian, Windows 2008, 2012, 2016, 7, 8, 8.1, 10 a MacOS);
- integraci zálohovacího řešení pro zálohování snapshotů a clonů na diskovém poli HP 3PAR a IBM Storwize v7000, včetně vytváření a práce s daty uvnitř těchto snapshotů pomocí zálohovacího prostředí (například data ze snapshotů budou využita pro zálohy, ale i obnovu pro kritické RTO a RPO) ve spolupráci s virtualizovaným prostředím VMware.

Vyžadujeme zajištění aplikační konzistence pro Oracle, MS SQL, VMware vSphere6, MS Exchange 2016 a souborové systémy Windows a Linux, volitelně GroupWise;

- dostatečný výkon celého řešeni, kdy požadavek na BTO a TO je - Maximální doba zálohy pro 1 TB zdrojových dat bude 1 hodina (při maximální paralelizaci 1). Očekávaná doba je 30 minut;
- centrální (globální) deduplikaci s podporou deduplikace na klientech zálohovacího prostředí. Deduplikace bude dostupná pro všechny zmíněné funkce a bude deduplikovat všechna data napříč celým řešením a dostupnou funkcionalitou včetně ukládání na pásky LTO;
- jednotný management (jednotnou konzoli) pro správu a konfiguraci celého prostředí
- (zálohování, archivace, replikace, řízení snapshotů diskových polí, správa účtů, granulární obnova);
- podpora efektivního zálohování poboček nebo vzdálených zařízení (vyžadujeme deduplikaci na zdroji a nezávislost na odezvách zálohovacích linek – tedy odezvy 500ms a více nesmí být překážkou pro provedení zálohy). Požadovaná je výše zmíněná replikace deduplikovaných dat do cloud úložiště (datacentra) a podpora obnovy dat včetně „bare-metal-recovery“ obnovy v záložní lokalitě;
- podporu Monitoringu a Reportingu v rozsahu
    - přístup a možnost kontrolovat prostředí zálohování a archivace. Požadujeme auditování přístupů do zálohovacího a archivačního prostředí, vytvoření definovaných přístupů našich administrátorů s možností provádět obnovy i zálohy celého prostředí. Vzhledem k rozsahu prostředí požadujeme definici přístupů tak, aby konkrétní administrátor zadavatele mohl pouze zálohovat, archivovat, měnit či vytvářet zálohy a obnovovat data a systémy, které spravuje a to i na úrovni databází, aplikací a OS
    - automatické vytváření denního a měsíčních reportu o stavu zálohování a o všech provedených změnách poskytovatelem;
- nativní podpora online zálohování databázových a aplikačních systémů pro Oracle ASM, Oracle RAC cluster, Microsoft Exchange, Sharepoint, Active Directory, GroupWise, MySQL a MSSQL a nativní zálohování image virtuálních serverů Vmware, XEN a KVM;
- aktivní podpora CDP/CDR (Continuous Data Protection a Continuous Data Replication) pro data uložena na fibre-channel diskových oblastech libovolných výrobců diskového pole a to primárně pro Oracle databázi a GroupWise data. Možnost okamžité replikace uložených kritických dat;
- v rámci IT infrastruktury zadavatel poskytne účastníkovi 4 x 10Gb port na LAN switchi, 4 x FC 8Gb port na SAN switch a 8 x LAN 1Gb.

4.3 Požadavky na zachování integrity se současným řešením zálohování a archivace zadavatele

Zadavatel využívá ve svém centrálním zálohovacím systému řešení Commvault Data Protection verze 11. V případě změny zálohovacího systému zadavatel požaduje u platných záloh s retencí delší než jeden měsíc provést účastníkem převod/migraci zazálohovaných dat do nabízeného řešení z důvodu udržení kontinuity zálohovaných dat. Předpokládaná kapacita dat pro migraci je 600 TB nekomprimovaných dat. Data jsou uložena na páskách LTO6/7 a v deduplikačním disku spravovaném systémem Commvault. Správnost migrace požadujeme otestovat zkušební obnovou VMware image, Oracle DB a granulární obnovou souborů z VMware Image.

Zadavatel požaduje potvrzení kompatibility dodávaného řešení v oblasti integrace se systémy VMware, Oracle RAC, HP 3PAR, IBM Storwize v7000, Microfocus GroupWise, MS Exchange 2016 a cloud úložišti. Zadavatel uvede URL adresu na stránkách výrobce nabízeného řešení, kde je možné požadovanou kompatibilitu ověřit.

Zadavatel požaduje vyjádření výrobce nabízeného řešení, jakým způsobem splňuje a řeší legislativu Evropské unie v oblasti ochrany osobních údajů - General Data Protection Regulation. Zadavatel uvede URL adresu na stránkách výrobce nabízeného řešení, kde je možné požadované vyjádření GDPR ready získat.

Požadavky na servisní podporu a SLA

1. **Činnosti servisní podpory zajišťované dodavatelem:**
    a) Pravidelná denní kontrola zálohovacího prostředí
    b) Automatické aktualizace patchů a servis packů
    c) Konfigurace nových požadavků záloh a přístupů
    d) Provádění krátkých testovacích obnov
    e) Požadovaná reálná obnova administrátora
    f) Pravidelný měsíční report + analýza dat v záloze
    g) Kontrola snapshotů a replikací dat diskových polí
    h) Testování Disaster Recovery a Instant Recovery
    i) Podpora zálohování koncových zařízení
    j) Konzultace

Dodavatel předloží vlastní návrh časové náročnosti jednotlivých položek servisních služeb zahrnující výše uvedené činnosti, ale trvá na minimální hodnotě 32 hodin a maximální hodnotě 64 hodin. Počet hodin servisní podpory je hodnotícím kritériem viz zadávací dokumentace**.**

2. **Hlášení servisních požadavků**
    - Přijímání servisních požadavků telefonicky, emailem a pomocí Heldesk portálu přístupného z internetu.
    - Helpdesk portál umožnuje vytvořit pro zadavatele uživatelské účty pro přihlášení do portálu a zadávání servisních požadavků
    - Helpdesk portál umožnuje kontrolu průběhu řešení (jednotlivých stavů) servisních požadavků zadavatele.
    - Helpdesk portál umožňuje nahrávání souborů (logy, reporty, apod.) potřebných k případné diagnostice poruch

3. **SLA v rámci služby zálohování**

Parametr	**Hodnota**
Dostupnost infrastruktury režimu 24x7	**99 %**

SLA řešení incidentů (response / fixtime)	
kritický	**2h/8h**
urgentní	**4/16 h**
méně závažný	**16/- h**
Helpdesk portál	**24/7**
Hotline	**24/7**
Monitoring systému	**24/7**

4. **Kritický incident**

   Kritickým incidentem se ve smyslu této smlouvy se rozumí stav celkové nefunkčnosti nebo nemožnosti využívání klíčových funkcionalit zařízení nebo systému. Uživatelé systému nemohou v takovém případě využívat služeb, které má systém poskytovat. Typicky se jedná o nefunkční zálohování kritických dat, nefunkční obnova souborů nebo emailových zpráv apod.

5. **Urgentní incident**

   Urgentním incidentem se ve smyslu této smlouvy rozumí takový stav zařízení či systému, kdy je některá komponenta nebo součást systému mimo provoz či neplní svoji funkci, ale systém jako celek je stále schopen alespoň omezeně poskytovat své služby či plnit svou funkcionalitu. Uživatelé mohou v takovém případě stále využívat služeb systému. Příkladem vážné poruchy bývá zpravidla výpadek některé redundantní komponenty zařízení (např. disk, řadič, zdroj, apod.) nebo celého zařízení, které tvoří součást clustrového řešení.

6. **Méně závažný incident**

   Méně závažným incidentem se ve smyslu této smlouvy rozumí takový stav zařízení nebo systému, který neodpovídá předávací dokumentaci, ale neohrožuje klíčové funkcionality řešení.