SNAS SLOVENSKÁ NÁRODNÁ AKREDITAČNÁ SLUŽBA
Karloveská 63, P. O. Box 74, 840 00 Bratislava 4

METODICKÁ SMERNICA PRE SPRÁVNU LABORATÓRNU PRAX

SLP A CLOUD COMPUTING

(Doplnok 1 k OECD Guideline No. 17 APLIKÁCIA ZÁSAD SLP NA POČÍTAČOVÉ SYSTÉMY)

MSA-G/17A

Vydanie: 1
Aktualizácia: 0

BRATISLAVA
Apríl 2024

Táto metodická smernica je prekladom dokumentu OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring,
Advisory Document on GLP & Cloud Computing
Supplement 1 to Document Number 17 on Application of GLP Principles to Computerised Systems.
ENV/CBC/MONO(2023)27

Spracoval: *Ing. Henrieta Bóriková*
Ing. Kvetoslava Forišeková

Preskúmal: *RNDr. Lívia Kijovská, PhD.*

Schválil:. *Ing. Štefan Král, PhD.*

Účinnosť od: *30.4.2024*

Táto MSA neprešla jazykovou úpravou.

Dostupnosť MSA: https://www.snas.sk

OBSAH

Strana

1 ÚVODNÉ USTANOVENIA

1.1 PREDHOVOR

Tento poradný dokument vypracovala Pracovná skupina OECD pre správnu laboratórnu prax (SLP). Vypracovanie dokumentu prebiehalo pod vedením Belgicka a Francúzska (Medical Products) a v spolupráci so zástupcami návrhovej skupiny z Austrálie, Rakúska, Dánska (Medical Products), Izraela, Japonska (Medical Products), Poľska, Švajčiarska, US-EPA a US-FDA. Dokument bol preskúmaný a schválený pracovnou skupinou pre správnu laboratórnu prax (SLP).

Za zverejnenie tohto dokumentu zodpovedá Výbor pre chemikálie a biotechnológiu, ktorý v júni 2023 jeho zverejnenie odsúhlasil.

2 DEFINÍCIA POJMOV

Prevzaté z OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No.1, OECD Principles of Good Laboratory Practice (as revised in 1997) a doplnené z ostatných doteraz vydaných Guidelines.

Pozn. SNAS: Vysvetlenie špecifických pojmov je uvedené v príslušných MSA-G, ktorých sa to týka.

2.1 SLP

Zásady správnej laboratórnej praxe – systém kvality vzťahujúci sa na proces organizácie a podmienky, za ktorých sa neklinické štúdie plánujú, vykonávajú, overujú, zaznamenávajú, ukladajú a oznamujú. Neklinické štúdie sa vykonávajú na testovacích pracoviskách, ktorými sú laboratóriá, skleníky a polia.

Národný program dodržiavania zásad SLP (NP SLP) – zisťuje, či testovacie pracoviská zaviedli zásady SLP do praxe a či sú schopné zabezpečiť, že výsledné údaje majú zodpovedajúcu kvalitu. NP SLP vymedzuje pôsobnosť a rozsah programu, poskytuje informáciu o mechanizme, prostredníctvom ktorého testovacie pracovisko vstúpi do programu, o druhoch inšpekcií testovacích pracovísk a auditov štúdií, opisuje rôzne druhy inšpekcií, ako aj ich frekvenciu a vymedzuje právomoci inšpektorov.

Osvedčenie SLP – je dokument, ktorým sa deklaruje, že testovacie pracovisko (laboratórium) vykonáva štúdie (testy, skúšky) v súlade so zásadami správnej laboratórnej praxe.

Národná monitorovacia autorita v dokumentoch OECD a EC = akreditujúca osoba (SNAS) v legislatíve SLP na Slovensku

2.2 POJMY TÝKAJÚCE SA TESTOVACIEHO PRACOVISKA

Testovacie pracovisko – pracovisko uvedené v zákone[1] vrátane osôb, priestorov a prevádzkových jednotiek potrebných na vykonávanie neklinických štúdií zdravotnej a environmentálnej bezpečnosti. Pre multicentrové štúdie, teda také, ktoré sú vykonávané

[1] § 2 písm. e) zákona č. 67/2010 Z.z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon).

na viacerých miestach, sa pod testovacím pracoviskom rozumie miesto, kde pracuje vedúci štúdie spolu so všetkými ďalšími testovacími miestami zúčastňujúcimi sa na štúdii.

Testovacie miesto – znamená také miesto, kde je vykonávaná určitá časť štúdie.

Vedenie testovacieho pracoviska (Test Facility Management – TFM) – osoba(y), ktorá je zodpovedná za organizáciu a chod testovacieho pracoviska podľa zásad správnej laboratórnej praxe. Vykonáva právne úkony, administratívno-správne úkony vo všetkých veciach testovacieho pracoviska na základe zmluvy o zriadení pracoviska zakladajúcou listinou alebo zákonom.

Vedenie testovacieho miesta – (ak bolo vymenované) – osoba(y) zodpovedajúca za to, aby časť štúdie, za ktorú zodpovedá, bola vykonávaná v súlade so zásadami SLP.

Vedúci testovacieho pracoviska – v prípade zložitejšej organizačnej štruktúry testovacieho pracoviska osoba, ktorá je priamo zodpovedná za konkrétnu činnosť testovacieho pracoviska podľa zásad správnej laboratórnej praxe (riaditeľ odboru, vedúci laboratória...). Právomoci na zabezpečenie činnosti podľa zásad SLP má delegované od vedenia testovacieho pracoviska buď poverením alebo definovaním v pracovnej náplni.

Objednávateľ štúdie – subjekt, ktorý si objednáva, finančne zabezpečuje a predkladá neklinickú štúdiu zdravotnej a environmentálnej bezpečnosti na posúdenie.

(Pozri aj Nariadenie vlády č. 320/2010 Z. z. v znení neskorších predpisov, § 3, (5)).

Pozn.:
Objednávateľom môže byť:

- *Subjekt*, ktorý prichádza s návrhom vykonať a podporuje, poskytnutím finančných alebo iných zdrojov, neklinické štúdie zdravotnej a environmentálnej bezpečnosti;*
- *Subjekt*, ktorý predkladá neklinické štúdie zdravotnej a environmentálnej bezpečnosti oprávnenej autorite pri registrácii produktu, alebo pri inej žiadosti, pre ktorú je súlad so zásadami SLP vyžadovaný.*

* *„Subjektom" môže byť jednotlivec, obchodná spoločnosť, združenie, vedecký, alebo akademický ústav, vládna agentúra alebo ich organizačné jednotky, alebo akýkoľvek iný právne identifikovateľný subjekt.*

Vedúci štúdie – osoba zodpovedajúca za celkové vykonanie neklinickej štúdie bezpečnosti zdravia a životného prostredia, vrátane plánu štúdie a záverečnej správy.

Vedúci čiastkovej štúdie – osoba, ktorá v prípade štúdie vykonávanej na viacerých miestach koná v mene vedúceho štúdie a zodpovedá za jemu pridelené časti štúdie.

Program zabezpečenia kvality (Quality Assurance Programme – QAP) – definovaný systém, zahŕňajúci zamestnancov, ktorý je nezávislý od vykonávania štúdie a slúži na zabezpečenie súladu postupu prác v testovacom pracovisku so zásadami správnej laboratórnej praxe.

Zabezpečenie kvality/Quality Assurance (QA): zdroje zodpovedné za implementáciu a udržiavanie QAP.

Pozn.: Zodpovednosti QA v SLP, okrem iného, nezahŕňajú riadenie dokumentácie systému kvality, riadenie nástrojov pre vylepšenia organizačných procesov (hoci niektoré testovacie pracoviská môžu prideliť tieto činnosti QA), schvaľovanie odchýlok alebo schvaľovanie primeranosti zdrojov. Uznáva sa, že iné systémy kvality (napr. ISO 9000, Správna výrobná prax (GMP), ISO 17025) používajú pojem „zabezpečenie kvality" v inom kontexte.

Štandardné pracovné postupy (ŠPP) – sú dokumentované postupy, ktoré opisujú, ako vykonávať testy alebo činnosti, ktoré nie sú detailne špecifikované v plánoch štúdií alebo v oficiálnych a všeobecne akceptovaných testovacích metódach (OECD, REACH).

Master Schedule – súbor informácií o vykonávaných štúdiách na testovacom pracovisku, slúži na sledovanie štúdií a vyťaženosti testovacieho pracoviska.

2.3 POJMY TÝKAJÚCE SA NEKLINICKÝCH ŠTÚDIÍ ZDRAVOTNEJ A ENVIRONMENTÁLNEJ BEZPEČNOSTI

Neklinická štúdia zdravotnej a environmentálnej bezpečnosti – ďalej len „štúdia“ – znamená experiment alebo súbor experimentov, ktorými je testovaná látka skúmaná v laboratórnych podmienkach alebo v životnom prostredí, s cieľom získať údaje o jej vlastnostiach a/alebo zdravotnej a environmentálnej bezpečnosti, ktoré sú plánované ako podklad pre rozhodnutie príslušnej regulačnej autority pred jej povolením do používania.

Krátkodobá štúdia – štúdia krátkeho trvania so všeobecne používanými bežnými technikami.

Multicentrová štúdia – akákoľvek štúdia, ktorej niektoré fázy sú vykonávané na viac ako jednom mieste. Takéto štúdie sú nevyhnutné, ak je potrebné využiť miesta, ktoré sú zemepisne vzdialené, organizačne rozdielne alebo ináč oddelené. To sa týka aj oddelenia organizácie, ktoré slúži ako testovacie miesto, kým iné oddelenie tej istej organizácie pôsobí ako testovacie pracovisko.

Fáza / etapa štúdie – definovaná činnosť alebo súbor činností pri uskutočňovaní štúdie.

Plán štúdie – dokument, ktorý definuje ciele a experimentálne plánovanie skúšok na vykonávanie štúdie, vrátane jeho zmeny a doplnkov.

Doplnok plánu štúdie – predstavuje cielenú zamýšľanú zmenu plánu štúdie.

Odchýlka od plánu štúdie – neočakávaná odchýlka od plánu štúdie po dátume začatia štúdie.

Testovací systém – biologický, fyzikálny alebo chemický systém alebo ich kombinácia použitá v štúdii.

Primárne údaje – všetky pôvodné záznamy a dokumentácia vypracovaná v testovacom pracovisku, alebo ich verifikované kópie, ktoré sú výsledkom pozorovaní a činností vykonaných v štúdii. Primárne údaje môžu zahŕňať aj fotografie, mikrofilmy, počítačové médiá na uchovávanie údajov, diktované pozorovania, záznamy z automatizovaných prístrojov alebo iné záznamové médiá určené na uchovávanie dát.

Vzorka – každý materiál odobratý z testovacieho systému za účelom vyšetrenia, analýzy alebo uchovávania.

Dátum začiatku štúdie – dátum, kedy vedúci štúdie podpísal plán štúdie.

Dátum experimentálneho začiatku štúdie – dátum, kedy boli získané prvé údaje zo štúdie.

Dátum ukončenia experimentu – posledný deň, kedy boli získané údaje zo štúdie.

Dátum ukončenia štúdie – dátum, kedy vedúci štúdie podpísal záverečnú správu zo štúdie.

2.4 POJMY TÝKAJÚCE SA TESTOVANEJ LÁTKY

Testovaná látka – látka, ktorá je predmetom SLP štúdie. Závery SLP štúdie poskytnú informácie o vlastnostiach testovanej látky, ktoré umožnia zhodnotiť, aké riziko predstavuje testovaná látka pre bezpečnosť ľudí, zvierat alebo pre životné prostredie.

Treba upozorniť že v niektorých OECD Test Guidelines sa pre „testovanú látku“ používa aj pojem "test chemical”. (odsúhlasené v júni 2013, OECD's Joint Meeting of the Chemicals Committee and the Working Party on Chemicals, Pesticides and Biotechnology). Teda môžeme sa stretnúť aj s pojmami "test item", "test compound", "test substance". Cieľom tohto návrhu nebolo zavedenie novej definície pojmu “chemikália”, ale skôr išlo o zosúladenie terminológie s definíciou uvedenou v UN GHS pre klasifikáciu a označovanie, kde sa pod chemikáliou myslí aj “látka a zmes”

Referenčná látka – akákoľvek látka, použitá ako základ na porovnanie s testovanou látkou.

Šarža – špecifické množstvo testovanej alebo referenčnej látky vyrobené v jednom cykle výroby, takým spôsobom, že sa dá očakávať, že látka má jednotný a homogénny charakter a dá sa za takú pokladať.

Nosič / Vehikulum – akákoľvek látka, ktorá slúži ako nosič na zmiešavanie, dispergovanie, vytvorenie suspenzie, alebo zvyšovanie rozpustnosti testovanej látky a/alebo referenčnej látky na uľahčenie jej podávania/aplikácie testovaciemu systému.

Formulácia (test. látka + nosič) – kombinácia testovanej látky a rôznych prísad, ako pomocných látok, ktoré sú skombinované a podávané a/alebo aplikované testovaciemu systému v rôznych formách (napr. tabletky, kapsule, roztok...).

Príprava testovanej látky/alebo pripravená testovaná látka – môže byť formuláciou (alebo zmesou) obsahujúcou testovanú látku, alebo testovanú látku v nosiči, kde sa táto kombinácia získa riedením, miešaním, dispergovaním, vytvorením suspenzie, rozpustením a/alebo iným procesom so zámerom aplikovať ju testovaciemu systému. Testovaciemu pracovisku môže byť dodaná testovaná látka (na priame podanie), alebo testovaná látka, ktorá ešte musí byť nejako pripravená alebo prípravok s testovanou látkou, ktorý možno priamo podať alebo aplikovať testovaciemu systému (tiež nazývaná “ready-to-use”).

Testovaná látka, ktorá je zapuzdrená (encapsulated) alebo balená iným spôsobom, bez prítomnosti pomocných látok alebo nosiča, sa nepovažuje za to isté ako „pripravená testovaná látka“ opisovaná v tomto dokumente.

Charakterizácia – určuje vlastnosti testovanej látky a poskytuje dôkazy na podporu vhodnosti jej použitia v SLP štúdiách.

Identifikácia – proces kontroly a hodnotenia testovanej látky porovnaním s dodanými informáciami, s cieľom určiť, či testovaná látka je tá, ako bola očakávaná. Poskytnutými informáciami môžu byť prepravné doklady, e-maily od dodávateľa, označenie etiketou na testovanej látke, atď. Typickými znakmi používanými na identifikáciu testovanej látky môžu byť – názov, číslo šarže, čistota, koncentrácia, zloženie, chemické, fyzikálne a biologické parametre. Identifikácia môže tiež zahŕňať fyzikálnu a/alebo analytickú kontrolu. Proces identifikácie musí byť vykonaný pred začiatkom experimentálnej fázy SLP štúdie.

Dátum exspirácie – stanovený dátum, do ktorého sa očakáva, že testovaná látka si zachová svoje vlastnosti v rámci špecifikácií, pokiaľ je skladovaná za definovaných podmienok a po uplynutí ktorého už nemôže byť použitá.

Dátum retestovania – dátum, kedy testovaná látka môže byť znovu otestovaná, s cieľom ubezpečiť sa, že je ešte stále vhodná na použitie.

2.5 POJMY TÝKAJÚCE SA INŠPEKCIE TESTOVACIEHO PRACOVISKA

Inšpekcia testovacieho pracoviska – kontrola postupov testovacieho pracoviska a praktických činností smerujúcich k dosiahnutiu stupňa zhody so zásadami SLP, počas ktorej sa skontrolujú systémy riadenia a pracovné postupy testovacieho pracoviska, ako aj integrita údajov, aby sa zabezpečilo, že výsledné údaje majú náležitú kvalitu na posúdenie a rozhodovanie národnými regulačnými orgánmi.

Inšpektor – osoba, vykonávajúca inšpekcie testovacích pracovísk a audity neklinických štúdií v zastúpení akreditujúcej osoby (SNAS).

Audit štúdií – porovnanie prvotných údajov a súvisiacich záznamov v predbežnej alebo záverečnej správe, s cieľom určiť, či primárne údaje boli presne zaznamenané, či sa testovanie vykonalo v súlade s plánom štúdie a štandardnými pracovnými postupmi, získať dodatočné informácie neuvedené v správe a stanoviť, či postupy použité pri spracovaní údajov mohli ovplyvniť ich validitu.

Správa o inšpekcii – oficiálny písomný doklad o vykonanej inšpekcii, v ktorej sú identifikované všetky posudzované prvky a činnosti, menovite uvedené všetky nedostatky a posúdená miera dodržiavania zásad SLP. Určuje kvalitu a integritu údajov preverovaného testovacieho pracoviska.

3 SKRATKY

GLP	Good Laboratory Practice
MSA	Metodická smernica na akreditáciu
OECD	(Organisation for Economic Cooperation and Development) Organizácia pre hospodársku spoluprácu a rozvoj
SLP	Správna laboratórna prax
SNAS	Slovenská národná akreditačná služba
ŠPP	Štandardný pracovný postup
SR	Slovenská republika
ÚZK	Útvar zabezpečenia kvality
NP SLP	Národný program dodržiavania zásad SLP
TFM	Vedenie testovacieho pracoviska (Test Facility Management)
QAP	Program zabezpečenia kvality (Quality Assurance Programme)
REACH	Európska chemická legislatíva - REACH (Registration, Evaluation, Authorisation of Chemicals)

4 SÚVISIACE PREDPISY

SR

Zákon 67/2010 Z. z. o podmienkach uvedenia chemických látok a chemických zmesí na trh a o zmene a doplnení niektorých zákonov (chemický zákon)

Nariadenie vlády č. 320/2010 Z. z., ktorým sa upravujú činnosti testovacích pracovísk a činnosti inšpektorov vykonávajúcich inšpekcie, audit a overovanie dodržiavania zásad správnej laboratórnej praxe.

Nariadenie vlády SR č. 92/2012 Z. z., ktorým sa mení a dopĺňa nariadenie vlády Slovenskej republiky č. 320/2010 Z. z., ktorým sa upravujú činnosti testovacích pracovísk a činnosti inšpektorov vykonávajúcich inšpekcie, audit a overovanie dodržiavania zásad správnej laboratórnej praxe**.**

Zákon č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody

MSA série G - všetky MSA vydané SNAS, týkajúce sa SLP dostupné na webovej stránke www.snas.sk

EU

Smernica 2004/9/ES o inšpekcii a overovaní správnej laboratórnej praxe (kodifikovaná verzia)

Smernica 2004/10/ES o zosúlaďovaní zákonov, predpisov a správnych opatrení uplatňovaných na zásady správnej laboratórnej praxe a overovanie ich uplatňovania pri testoch chemických látok (kodifikovaná verzia)

Nariadenie Európskeho parlamentu a Rady (ES) č. 1907/2006 z 18. decembra 2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemikálií **(REACH)** a o zriadení európskej chemickej agentúry (ECHA), o zmene a doplnení smernice 1999/45/ES a o zrušení nariadenia Rady (EHS) č. 793/93 a nariadenia Komisie (ES) č. 1488/94, smernice rady76/769/EHS a smerníc Komisie 91/155/EHS, 93/67/EHS, 93/105/ES A 2000/21/ES, v platnom znení.

Nariadenie Európskeho parlamentu a Rady (ES) č. 1272/2008 zo 16. decembra 2008 o klasifikácii, označovaní a balení látok a zmesí, o zmene, doplnení a zrušení smerníc 67/548/EHS a 1999/45/ES a o zmene a doplnení nariadenia (ES) č. 1907/2006, platnom znení.

Nariadenie Komisie č. 440/2008 z 30. mája 2008, ktorým sa ustanovujú testovacie metódy podľa nariadenia EP a R č. 1907/2006 o registrácii, hodnotení, autorizácii a obmedzovaní chemických látok **(REACH).**

OECD

1981 Council Act Decision [C (81)30/Final] on the Mutual Acceptance of Data in the Assessment of Chemicals,

1989 Council Decision Recommendation on Compliance with Principles of Good Laboratory Practice [C (89)87/Final],

5 VECNÁ ČASŤ

5.1 HISTÓRIA

Zásady správnej laboratórnej praxe (SLP) vyžadujú, aby záznamy a materiály, vrátane elektronických záznamov a údajov potrebných na rekonštrukciu neklinických štúdií, spĺňali požiadavky na kvalitu, integritu a dostupnosť údajov a boli riadne uchovávané a archivované.

Na splnenie týchto požiadaviek využíva čoraz väčší počet testovacích pracovísk cloudové aplikácie. Pri používaní cloudových aplikácií je však potrebné zvážiť ich vplyv na dodržiavanie

zásad SLP. Testovacie pracoviská majú konečnú zodpovednosť za súlad so zásadami SLP pri posúdení rizík na integritu, kvalitu, dostupnosť, uchovávanie a archiváciu údajov.

Cloud označuje poskytovanie sieťového prístupu na požiadanie k zdieľanému fondu konfigurovateľných výpočtových zdrojov používateľom a môže zahŕňať softvér, siete/platformy alebo infraštruktúru. Cloudové riešenia v SLP pokrývajú externý vývoj, údržbu a prevádzkovanie výpočtovej techniky v priestoroch testovacieho pracoviska alebo mimo nich,
ako napríklad:

1. Hardvér alebo servery prepojené sieťami.
2. Softvér alebo aplikácie, ktoré zachytávajú, generujú, analyzujú, migrujú, ukladajú, archivujú údaje.
3. Rozhrania medzi aplikáciami.
4. Databázy.

5.2 ÚVOD

Tento dokument opisuje požiadavky orgánov monitorujúcich dodržiavanie SLP na testovacie pracoviská, ktoré používajú cloudové riešenia.

Cloudová služba sa môže podieľať na zbere, spracovaní, ukladaní a archivovaní SLP údajov.

Tento dokument sa zameriava na špecifické vlastnosti cloudových riešení, najmä na spoluprácu medzi testovacím pracoviskom a poskytovateľom cloudových služieb a objasňuje požiadavky zásad SLP, ktoré sa musia uplatňovať.

Tento dokument sa považuje za doplnok k dokumentu OECD Guideline No. 17 (Aplikácia zásad SLP na počítačové systémy) (OECD, 2016[1]) a mal by sa čítať a uplatňovať v spojení s dokumentmi OECD Guideline No. 1 (Zásady SLP) (OECD, 1997[2]), OECD Guideline No. 15 (Zriadenie priestorov na uchovávanie v súlade so zásadami SLP) (OECD, 2007[3]), OECD Guideline No. 5 (Súlad laboratórnych dodávateľov so zásadami SLP) (OECD, 2002[4]) a OECD Guideline No. 22 (Integrita údajov) (OECD, 2021[5]) a príslušných národných predpisov.

5.3 ROZSAH PÔSOBNOSTI

Cloudové služby môžu byť interne poskytované služby testovacieho pracoviska alebo spoločnosti, do ktorej testovacie pracovisko patrí, alebo externé služby poskytované zmluvnými poskytovateľmi IT služieb. Po uzatvorení zmluvy môže byť služba poskytovaná priamo poskytovateľom cloudových služieb alebo prostredníctvom predajcu. Poskytovatelia služieb môžu mať aj subdodávateľov pre celú službu alebo jej časť. Tento dokument sa vzťahuje na všetky typy služieb.

Poznámka: Pojem „poskytovateľ cloudových služieb“ sa v tomto dokumente používa pre všetky typy poskytovateľov cloudových služieb vrátane interného IT, externého IT, poskytovateľa hosťovaných služieb, predajca (zvyčajne fyzická osoba alebo subjekt, ktorý služby predáva), dodávateľa (zvyčajne ten ktorého úlohou je poskytovať požadované služby) alebo poskytovateľ cloudu.

Dokument sa vzťahuje na všetky cloudové riešenia vrátane tých, ktoré sa už používajú.

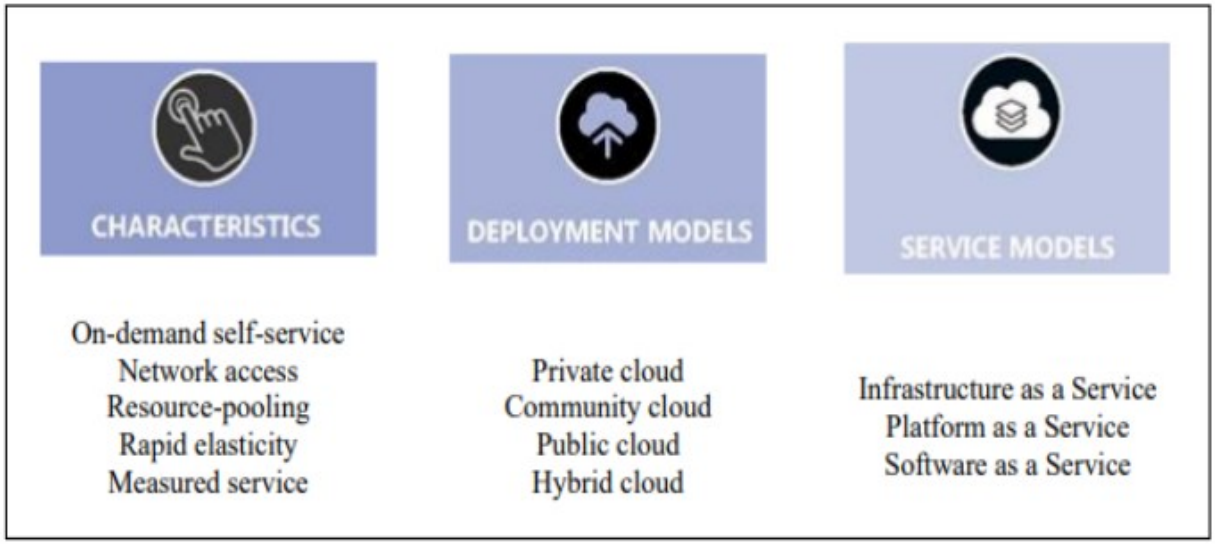
Požiadavky v tomto dokumente pre „testovacie pracovisko“ a „Manažment testovacieho pracoviska (TFM)“ sa rovnako vzťahujú na „testovacie miesto“ a „Manažment testovacieho miesta“.

5.4 PREHĽAD O „CLOUD COMPUTING“

5.4.1 Definícia

Vo všeobecnosti možno cloud computing definovať ako model, ktorý na požiadanie umožňuje sieťový prístup k zdieľanému fondu konfigurovateľných počítačových zdrojov. Americký Národný inštitút pre štandardy a technológie (NIST) (Peter Mell, 2011[6]) definuje cloud computing ako „model umožňujúci všadeprítomný, pohodlný sieťový prístup na požiadanie k zdieľanému fondu konfigurovateľných počítačových zdrojov (napr. siete, servery, úložiská, aplikácie a služby), ktoré je možné rýchlo, s minimálnym úsilím a bez potreby interakcie s prevádzkovateľom služby poskytnúť a zase uvoľniť.“ Podľa NIST cloud computing má päť základných charakteristík, štyri modely nasadenia a tri modely služieb, ako je opísané na obrázku 1.

Obrázok 1. Charakteristiky cloud computingu, spôsoby jeho nasadenia a poskytovaných služieb.



Zdroj: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[7])

Legenda k tabuľke:

Characteristics – Charakteristiky:
- *On-demand self-service - Samoobslužné služby na požiadanie*
- *Network access - Sieťový prístup*
- *Resource-pooling - Združovanie zdrojov*
- *Rapid elasticity - Rýchla elasticita*
- *Measured service - Meraná služba*

Deployment models - Modely nasadenia:
- *Private cloud - Súkromný cloud*
- *Community cloud - Komunitný cloud*
- *Public cloud - Verejný cloud*
- *Hybrid cloud - Hybridný cloud*

Service models - Modely služieb

Infrastructure as a Service (IaaS) - Infraštruktúra ako služba
Platform as a Service (PaaS) - Platforma ako služba
Software as a Service (SaaS) - Softvér ako služba

Tieto charakteristiky, spôsoby nasadenia a poskytovaných služieb, ako ich definuje NIST, sú uvedené alebo parafrázované nižšie. Možné príklady využitia v SLP sú uvedené ďalej v texte (pozri časť 5.4.3 a časť 5.4.4).

5.4.2 Charakteristiky

Základnými charakteristikami cloud computingu sú samoobslužné služby na požiadanie, širokopásmový prístup k sieti, združovanie zdrojov, rýchla elasticita (t. j. ľahká prispôsobiteľnosť a flexibilita) a meranie využívania služby.

1. **Samoobslužné služby na požiadanie / On-demand self-service:** Používatelia majú k dispozícii výpočtové zdroje bez akejkoľvek ľudskej interakcie s poskytovateľom služieb.
2. **Sieťový prístup / Network access:** Výpočtové zdroje sú dostupné cez sieť, podporujúce heterogénne klientske platformy (napr. mobilné zariadenia a pracovné stanice).
3. **Združovanie zdrojov / Resource-pooling:** Výpočtové zdroje poskytovateľa sa združujú, aby slúžili viacerým používateľom pod modelom jedného alebo viacerých nájomcov s rôznymi fyzickými a virtuálnymi zdrojmi (napr. úložisko, spracovanie, pamäť a šírka pásma siete), ktoré sú dynamicky priraďované a preraďované podľa požiadaviek užívateľa.
4. **Rýchla elasticita (škálovateľnosť) / Rapid elasticity (scalability):** Kapacity môžu byť elasticky zabezpečované a uvoľnené, v niektorých prípadoch automaticky, aby sa rýchlo rozširovali smerom von a dovnútra, primerane dopytu.
5. **Merateľná služba / Measured service:** Cloudové systémy optimalizujú využitie zdrojov vhodným využívaním a meraním poskytovaných kapacít podľa typu služby (napr. aktívne používateľské účty). Využívanie zdrojov je možné monitorovať, merať, kontrolovať a hlásiť, poskytujúc transparentnosť pre poskytovateľa a užívateľa (platba za použitie).

5.4.3 Modely zavádzania

Cloud computing je možné použiť v rôznych modeloch podľa typu použitia. Existujú štyri typy modelov: súkromné, verejné, komunitné a hybridné (obrázok 2.).
Hlavné rozdiely medzi týmito modelmi nasadenia sa týkajú dostupnosti cloudovej infraštruktúry:

1. **Súkromný cloud / Private cloud:** Cloudová infraštruktúra je poskytovaná na výhradné použitie jednou organizáciou, ktorá pozostáva z viacerých používateľov (napríklad obchodných jednotiek). Môže ho vlastniť, spravovať a prevádzkovať organizácia, tretia strana alebo ich kombinácia. Infraštruktúra cloudu je spravidla umiestnená mimo priestorov organizácie, ale umiestnenie údajov je pod kontrolou organizácie.

   V SLP súkromný cloud znamená hosťovanie výpočtových zdrojov výlučne pre potreby zmluvného testovacieho pracoviska alebo organizácie, ktorej patrí. K tomu dochádza v rámci súkromnej internej siete alebo tam, kde je infraštruktúra vyhradená zmluvnému testovaciemu pracovisku s úplne izolovaným prístupom bez ohľadu na to, či ju poskytuje externý alebo interný poskytovateľ cloudových služieb.

2. **Komunitný cloud / Community cloud:** Cloudová infraštruktúra je poskytovaná na výhradné použitie konkrétnej komunite používateľov z organizácií, ktoré majú spoločné požiadavky (napr. poslanie, požiadavky na bezpečnosť, zásady, hľadiská zhody pre testovacie pracoviská). Môže ju vlastniť, spravovať a prevádzkovať jedna alebo viacero organizácií v komunite, tretia strana alebo ich kombinácia. Infraštruktúra cloudu je spravidla umiestnená mimo priestorov organizácie.

   V SLP pre komunitný cloud platí, že cloudová infraštruktúra je zdieľaná niekoľkými testovacími pracoviskami, ktoré majú podobné záujmy (napr. pokiaľ ide o bezpečnosť, súlad). Prístup nie je verejný, ale je prístupný len pre definovanú skupinu užívateľov so spoločnými požiadavkami. Takýto cloud môže prevádzkovať jedna z týchto inštitúcií alebo tretia strana.

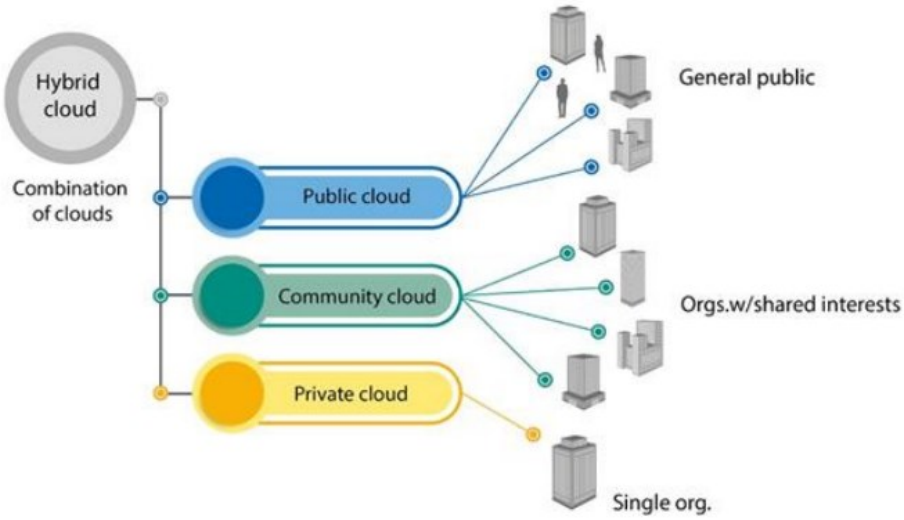
3. **Verejný cloud / Public cloud:** Cloudová infraštruktúra je poskytovaná na používanie širokej verejnosti. Môže ju vlastniť, spravovať a prevádzkovať firma, akademická alebo vládna organizácia, prípadne ich kombinácia. Existuje v priestoroch poskytovateľa cloudu. Presné umiestnenie fyzickej infraštruktúry, na ktorej sú uložené údaje, alebo spustené aplikácie, je používateľom spravidla neznáme.

   V SLP verejný cloud znamená hosťovanie výpočtových zdrojov, ktoré môže využívať široká verejnosť alebo veľká skupina, ako napríklad celé priemyselné odvetvie; tieto služby poskytuje príslušný poskytovateľ cloudových služieb vo svojich zariadeniach/dátových centrách.

4. **Hybridný cloud / Hybrid cloud:** Cloudová infraštruktúra je zložená z dvoch alebo viacerých rôznych cloudových infraštruktúr (súkromných, komunitných alebo verejných), ktoré zostávajú jedinečnými entitami, ale sú navzájom spojené štandardizovanou alebo proprietárnou technológiou, ktorá umožňuje prenosnosť údajov a aplikácií (napr. cloud bursting na vyrovnávanie záťaže medzi cloudmi). Ako príklady zmiešaných riešení založených na cloude je možné uviesť aplikáciu umiestnenú v časti verejného cloudu, ktorej dostupnosť a správa sú navrhnuté ako v súkromnom cloude pomocou bezpečnostných opatrení a obmedzení prístupu („súkromný cloud vo verejnom cloude“). Alebo je aplikácia umiestnená vo verejnom cloude a vygenerované údaje sa ukladajú a uchovávajú na serveroch testovacieho pracoviska (kombinácia verejného cloudu a tradičnej IT infraštruktúry).

Pre SLP hybridný cloud znamená kombináciu verejného a súkromného cloudu. Testovacie pracovisko využíva verejný cloud, ale má aj svoj vlastný súkromný cloud a môže medzi nimi vytvoriť prepojenie, aby fungovali ako jeden systém.

Obrázok 2. Modely nasadenia „Cloud computing“



Zdroj: FSI Insights on policy implementation No. 13, Regulating and supervising the clouds: emerging prudential approaches for insurance companies (Crisanto et al., 2018[7]).

Legenda k tabuľke:

Hybrid cloud - Hybridný cloud
Combnation of clouds - kombinácie cloudov
Public cloud - Verejný cloud
General public - Široká verejnosť
Community cloud - Komunitný cloud
Orgs.w/shared interests - Organizácie w/spoločné záujmy
Private cloud - Súkromný cloud
Single org. - Samostatné org.

5.4.4 Servisné modely

Modely služieb sa vzťahujú na typ ponúkaného výpočtového prostriedku. Existujú tri hlavné typy modelov služieb: infraštruktúra ako služba (IaaS), platforma ako služba (PaaS) a softvér ako služba (SaaS):

1. **Infraštruktúra ako služba / Infrastructure as a Service (IaaS):** Používateľ môže využívať službou poskytnuté zdroje ako napr. siete, úložiská dát a výpočtové zdroje, na ktorých môže používateľ nasadiť a spustiť ľubovoľný softvér, vrátane operačných systémov a aplikácií. Používateľ nespravuje ani neriadi základnú cloudovú infraštruktúru (napr. hardvér) a má obmedzenú až úplnú kontrolu nad operačnými systémami, úložiskom, nasadenými aplikáciami a sieťovými komponentmi (napr. hostiteľskými firewallami).

   Pre testovacie pracoviská ponúka služba IaaS hosťovanie a údržbu hardvéru a siete (fyzických aj virtuálnych komponentov) a dostupnosť úložnej a výpočtovej kapacity a zdrojov.

2. **Platforma ako služba / Platform as a Service (PaaS):** Používateľ môže nasadiť do cloudovej infraštruktúry ním vytvorené alebo získané aplikácie vyvinuté pomocou programovacích jazykov, knižníc, služieb a nástrojov podporovaných poskytovateľom cloudových služieb. Platforma ako služba je služba, pri ktorej externý dodávateľ dodáva okrem infraštruktúry aj platformu na vývoj aplikácií v cloude, ako je operačný systém,

middleware, databáza atď. Poskytovanie tejto služby zahŕňa správu infraštruktúry a základného aplikačného softvéru. Používateľ by bol zodpovedný za konfiguráciu aplikácie a jej vhodnosť na zamýšľané použitie.

V testovacích pracoviskách SLP sa poskytuje hardvér a prostredie. Platforma ponúka možnosť spravovať údaje a dokumentáciu. Súčasťou takýchto služieb sú často aj operácie ako migrácia, klasifikácia, ukladanie. Testovacie pracovisko SLP zostáva zodpovedné za konfiguráciu systémov a správu softvéru.

– *Príklad: Poskytovateľ cloudových služieb poskytuje aplikačný server a databázu, ktorá umožňuje implementáciu systému správy laboratórnych informácií (LIMS).*

3. **Softvér ako služba / Software as a Service (SaaS):** Používateľ má možnosť používať aplikácie poskytovateľa, ktoré bežia na cloudovej infraštruktúre. Aplikácie sú prístupné z rôznych klientskych zariadení prostredníctvom rozhrania, ako je napr. webový prehliadač alebo programové rozhranie. Používateľ nespravuje ani nekontroluje základnú cloudovú infraštruktúru vrátane aplikácií, siete, serverov, operačných systémov, úložiska, dokonca ani jednotlivé možnosti aplikácie, s možnou výnimkou obmedzených nastavení konfigurácie aplikácií špecifických pre používateľa.

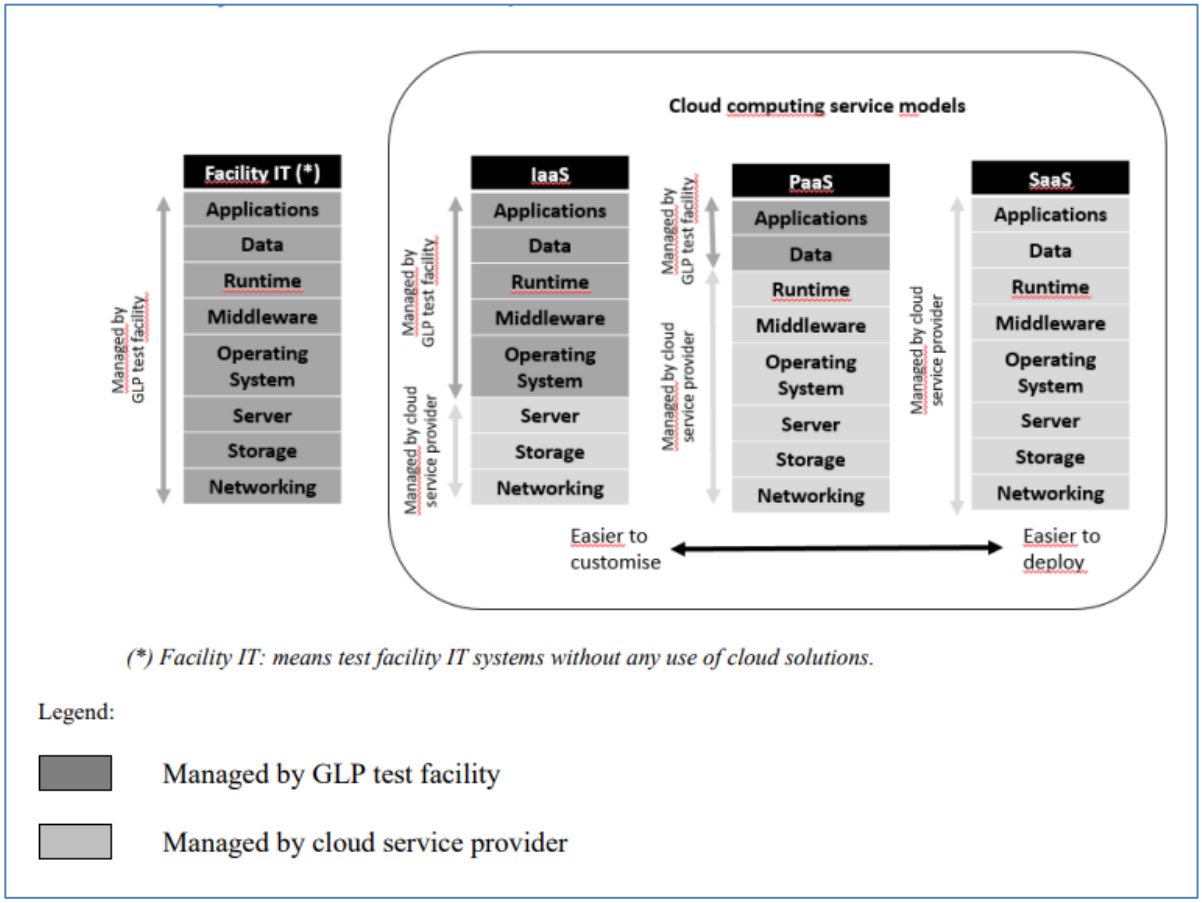
   V SLP model SaaS poskytuje testovaciemu pracovisku aplikácie, ktoré generujú alebo analyzujú údaje, ako aj spravujú dokumentáciu a ktoré vyvíja, inštaluje, udržiava a aktualizuje poskytovateľ cloudových služieb. Hardvér je zvyčajne umiestnený v dátovom centre (väčšinou vo verejnom cloude, aby sa umožnil prístup veľkému množstvu používateľov). Toto umiestnenie v dátovom centre je zvyčajne subdodávkou dodávateľa softvéru pre tretiu stranu. Celý návrh zabezpečenia zabezpečuje poskytovateľ cloudových služieb (spravidla prostredníctvom iných subdodávateľov). Testovacie pracovisko sa musí pri používaní softvéru pripojiť prostredníctvom spoločnej alebo zdieľanej platformy so špecifickými prístupovými právami. Súčasťou poskytovaných služieb je často aj školenie. Úroveň počítačového zásahu testovacieho pracoviska SLP je obmedzená na interné definovanie prístupov používateľov do systému. Zahŕňa aj konfiguráciu aplikácie na zamýšľané použitie testovacieho pracoviska vrátane bezpečnosti vo fáze implementácie. Používanie SaaS pozostáva z prepojenia s mechanizmom autentifikácie a zadávania údajov.

   – *Príklad: systém elektronických laboratórnych zápisníkov môže byť umiestnený vo verejnom cloude, čo umožňuje zachytávanie prvotných údajov na elektronických zariadeniach. Údaje sú priamo prenášané zo zariadení cez zabezpečenú sieť, aby boli uložené v súkromnej (zabezpečenej) oblasti, ktorá je tiež umiestnená vo verejnom cloude.*

4. **Desktop ako služba / Desktop as a Service (DaaS):** V porovnaní s modelom SaaS, poskytuje táto technológia aj prostredie desktopu. V tomto modeli sú všetky komponenty desktopu virtualizované a na prístup k virtuálnemu desktopu je potrebné len zariadenie.

Obrázok 3. poskytuje prehľad o tom, ako sa správa hlavných komponentov cloudového riešenia zvyčajne delí medzi testovacie pracovisko a poskytovateľa cloudových služieb v závislosti od zvolených modelov služieb cloud computingu.

Obrázok 3. Zdieľaná správa hlavných komponentov služby cloud computing medzi testovacím pracoviskom SLP a poskytovateľom cloudových služieb



Legenda k tabuľke:

Facility IT - IT testovacieho pracoviska**
(*) - znamená IT systémy testovacieho pracoviska bez použitia cloudových riešení.
Managed by GLP test facility – Spravované testovacím pracoviskom SLP – v obrázku vyznačené tmavosivou farbou

Cloud computing service models - Modely služieb cloud computingu (3 typy – stĺpce IaaS, Paas, SaaS)
Managed by cloud service provider – Spravované poskytovateľom cloudových služieb – v obrázku vyznačené svetlosivou farbou
Managed by GLP test facility – Spravované testovacím pracoviskom SLP – v obrázku vyznačené tmavosivou farbou

Applications - Aplikácie
Data - Údaje
Runtime – zaužívaný výraz aj v slovenčine, neprekladá sa
Middleware - zaužívaný výraz aj v slovenčine, neprekladá sa
Operating System - Operačný systém
Server - Server
Storage - Úložný priestor
Networking - Pripojenie do siete

Easier to customise - Jednoduchšie prispôsobenie
Easier to deploy - Jednoduchšie nasadzovanie

5.5 CLOUD COMPUTING V SLP

5.5.1 Zodpovednosti testovacieho pracoviska

Manažment pracoviska (TFM) je zodpovedný za dodržiavanie SLP v rámci testovacieho pracoviska a systémov, ktoré podporujú činnosti SLP. Ak sa operácie IT presunú z lokálne riadených serverov na cloudové riešenie je nevyhnutné, aby príslušné znalosti, informovanosť o systémoch a postupoch a dohľad nad nimi zostali v testovacom pracovisku a aby sa vykonávala kontrola. To platí bez ohľadu na to, či ide o interne spravovaný cloud (ako súčasť testovacieho pracoviska alebo ako súčasť organizácie, ktorej testovacie pracovisko patrí) alebo o externý cloud prostredníctvom externého poskytovateľa cloudových služieb.

Vzhľadom na komplexnosť ponúkanej služby sa tiež akceptuje, že TFM môže poveriť uzatváraním zmlúv a riadením takýchto služieb špecialistov alebo interné špecializované oddelenia zodpovedné za všeobecný výber dodávateľov, uzatváranie zmlúv a dohľad. Transparentnosť dohôd a povinnosti všetkých zúčastnených strán sú preto kľúčovým prvkom, ktorý umožňuje škálovateľnú úroveň detailov v závislosti od poskytovanej služby. Napriek tomu, aj keď sú úlohy delegované, TFM je stále zodpovedný za dodržiavanie zásad SLP v testovacom pracovisku.

Správca systému má prístup k aktuálnym a archivovaným údajom a dokumentom. Ak sú údaje umiestnené u poskytovateľa cloudových služieb, je potrebné definovať a objasniť okolnosti prístupu a činnosti vykonávané na údajoch. Práva správcu by nemali byť udelené osobám s potenciálnym záujmom o údaje a/alebo dokumentáciu. Je potrebné vypracovať a uplatňovať jasné stratégie na zmiernenie rizika a kontrolované postupy, aby sa zabezpečila integrita, kvalita a dostupnosť údajov, nezávisle od toho, kde sa nachádza správca systému (testovacie pracovisko alebo dodávateľ).

Vedúci štúdie musí zabezpečiť validáciu počítačových systémov (vrátane virtuálnych komponentov, ktoré môžu byť umiestnené lokálne alebo v cloude) používaných v štúdiách.

Za správu archívov zodpovedá archivár. Ak sú archívy SLP uložené v cloudovom riešení, archivár môže potrebovať využiť pomoc odborníkov na preskúmanie technických aspektov. Napriek tomu archivár zostáva zodpovedný a musí zabezpečiť, že:

1. Podmienky archivácie zabezpečujú integritu archivovaných elektronických záznamov.
2. Prístup k archívom je kontrolovaný.
3. Systém indexovania umožňuje systematické ukladanie a vyhľadávanie záznamov.
4. Migrácie archivovaných elektronických záznamov sú náležite kontrolované a dokumentované.
5. Je zavedený proces pravidelnej kontroly čitateľnosti a integrity údajov.
6. Je zavedený proces na zabezpečenie čitateľnosti údajov po ich migrácii z cloudového prostredia do testovacieho pracoviska (stratégia výstupu).

Program zabezpečenia kvality (QA) musí zabezpečiť zachovanie súladu so zásadami SLP. Používanie riešení založených na cloude v štúdiách SLP sa musí overiť z hľadiska ich súladu so zásadami SLP prostredníctvom kontroly kvality tak, ako pri iných počítačových systémoch.

5.5.2 Požiadavky

Požiadavky SLP na počítačové systémy a hosťované služby (alebo cloudové služby) sú opísané hlavne v dokumentoch OECD Guideline No. 1, No. 15 a No. 17. Tabuľka 1. poskytuje prehľad požiadaviek SLP špecifikovaných v dokumente OECD Guideline No. 1 vo vzťahu k rôznym modelom služieb cloud computingu.

Tabuľka 1. Riadenie požiadaviek SLP v rámci rôznych modelov cloudových služieb

Legenda k tabuľke:

Svetlošedá: pod plnou správou a intervenciou testovacieho pracoviska.
Tmavošedá: správa a intervencia je zdieľaná medzi testovacím pracoviskom a poskytovateľom cloudových služieb a prípadnými subdodávateľmi
Čierna: pod plnou správou poskytovateľa cloudových služieb.

Poznámka: Konečnou zodpovednosťou testovacieho pracoviska je posúdiť a preukázať, či cloudové služby dokážu zabezpečiť kvalitu, integritu a dostupnosť údajov a neovplyvnia súlad so zásadami SLP.

(*)Tradičné IT: znamená IT systémy testovacieho pracoviska bez použitia cloudových riešení

Computing resources *Zdroje výpočtovej techniky*	**Traditional IT** *Tradičné IT(*)*	**GLP Principles requirements** *Požiadavky zásad SLP*	**Cloud service models** *Servisné modely cloudov*		
			IaaS	**PaaS**	**SaaS**
Raw Data (including metadata) *Nespracované údaje (vrátane metadát)*		1.2.2.f, 1.4.3, 8.3.5			
Data generation *Generovanie údajov*					
Data classification and accountability *Klasifikácia údajov a zodpovednosť za ne*					
Protection *Ochrana*					
User access management *Správa prístupov používateľov*					
Encryption *Šifrovanie*					
Metadata, audit trail generation and management *Metadáta, vytváranie a správa auditných záznamov (audit trail)*					
Migration *Migrácia*		1.2.2.f, 1.4.3, 8.3.5			
Physical security measures for raw data *Fyzické bezpečnostné opatrenia pre nespracované údaj*e		1.2.2.i			
Application and software *Aplikácia a softvér*		1.1.2.b, 1.1.2.q, 1.2.2.g, 4.1			
Application level controls (access, rights) *Kontroly na úrovni aplikácií (prístup, práva)*					
Physical security measures for hosting of applications *Fyzické bezpečnostné opatrenia pre hosťovanie aplikácií*					

Computing resources *Zdroje výpočtovej techniky*	**Traditional IT** *Tradičné IT(*)*	**GLP Principles requirements** *Požiadavky zásad SLP*	**Cloud service models** *Servisné modely cloudov*		
			IaaS	**PaaS**	**SaaS**
Runtime (databases) *Doba bežania programu (databázy)*		1.1.2.q			
Middleware (interface betwen applications) *Softvér umožňujúci komunikáciu (rozhranie medzi aplikáciami)*		1.1.2.q			
Operating systems (Windows, Linux, etc.) *Operačné systémy (Windows, Linux atď.)*		1.1.2.b			
Virtualisation *Virtualizácia*		1.1.2.b			
Servers (account, application and data servers) *Servery (pre účty, aplikácie a údaje)*		1.1.2.b, 3.1.1			
Storage *Skladovanie*		1.1.2.b, 1.2.2.i, 3.1.1			
Backup and restore *Zálohovanie a obnovenie*		1.1.2.b, 1.2.2.i, 3.1.1			
Data archiving *Archivácia údajov*		1.1.2.b, 1.1.2.1, 1.1.2.q, 3.4, 9.2.7, 10			
Host infrastructure *Infraštruktúra hostiteľa*					
Physical security measures for hosting of archives *Opatrenia fyzickej bezpečnosti pri hosťovaní archívov*					
Networking (web browser, web server) *Siete (webový prehliadač, webový server)*		1.1.2.b			
VPN, firewall, and network security *Sieť VPN, brána firewall a zabezpečenie siete*					
Network control *Riadenie siete*					
Disater Recovery Plan (DRP) *Plán obnovy po havárii (DRP)*		1.1.2.b, 3.1.1, 3.4			
Retirement *Vyradeniie z prevádzky*		1.1.2.q, 10.4			
IT personnel *Pracovníci IT*		1.1.2.b,c,d, 1.4.1			
Computerised systems validation (and periodic review, change control) *Validácia počítačových systémov (a pravidelná kontrola, kontrola zmien)*		1.1.2.q, 1.2.2.g			
Quality Assurance (QA) *Zabezpečenie kvality*		1.1.2.f, 2.1.1, 2.1.2			

Testovacie pracovisko pri riadení poskytovateľov cloudovej služby musí spĺňať všetky požiadavky uvedené v dokumente OECD Guideline No. 17, časť „dodávateľ“ (oddiel 1.6, body 34 až 40).

V dokumente OECD Guideline No. 17 (odsek 39) sa uvádza, že s cloudovými alebo hosťovanými službami (napr. platforma, softvér, ukladanie údajov, archivácia, zálohovanie alebo procesy ako služba) sa musí zaobchádzať ako s akoukoľvek inou dodávateľskou službou a vyžadujú sa písomné dohody opisujúce úlohy a zodpovednosti každej strany.

Je zodpovednosťou TFM posúdiť príslušnú službu a odhadnúť riziká pre kvalitu, integritu a dostupnosť údajov. TFM si musí byť vedomý potenciálnych rizík vyplývajúcich z nekontrolovaného používania cloudových služieb a musí mať prostriedky na to, aby bol o týchto rizikách a ich vplyvoch na dodržiavanie SLP informovaný. Musia sa zaviesť a zdokumentovať vhodné opatrenia na zmiernenie rizík.

Poskytovatelia cloudových služieb môžu spolupracovať priamo alebo ako subdodávateľ od iného dodávateľa. TFM musí náležite kontrolovať všetkých dodávateľov relevantných pre SLP a činnosti subdodávateľa musia byť pre TFM transparentné. V písomných dohodách medzi testovacím pracoviskom a poskytovateľom cloudových služieb sa musí uvádzať, či sa časti služby môžu zadať subdodávateľom (pozri kap. 5.5.3.3 „Dohoda o úrovni služieb / Service Level Agreement (SLA)“).

5.5.3 Implementácia cloudového riešenia v SLP

Ak sa cloudové služby používajú na poskytovanie, inštaláciu, konfiguráciu, integráciu, kvalifikáciu, údržbu, úpravu alebo uchovávanie počítačového systému, nasledujúce štyri prvky zohrávajú kľúčovú úlohu pri zabezpečovaní súladu testovacieho pracoviska so zásadami SLP.

1. Podrobné posúdenie rizík (s opisom cloudového riešenia ako podmienkou).
2. Dôkladné posúdenie poskytovateľa cloudových služieb, vrátane auditov, ak je to relevantné, pred použitím a pravidelným preskúmaním.
3. Jasne definované dohody o úrovni služieb, ktoré priamo súvisia s prevádzkovými činnosťami a službami, ktoré sa majú poskytovať.
4. Validácia počítačových systémov umiestnených v cloudových službách.

   Poznámka: Pre fyzické a virtuálne servery platia rovnaké požiadavky.

5.5.3.1. Hodnotenie rizík a výber cloudových služieb

Riadenie rizík sa musí uplatňovať počas celého životného cyklu každého počítačového systému, pričom sa musí brať do úvahy kvalita údajov, integrita údajov a ich dostupnosť.

Predtým, ako sa TFM zaviaže ku cloudovému riešeniu sa musia identifikovať a opísať potenciálne spôsoby zlyhania, posúdiť súvisiace riziká pre súlad so zásadami SLP vrátane pravdepodobnosti a dopadu a navrhnúť účinné opatrenia na ich zmiernenie. Cloudové služby sa musia vyvíjať, uvoľňovať a spravovať tak, aby sa zabezpečila kvalita údajov, integrita údajov a dostupnosť údajov bez toho, aby sa ohrozilo dodržiavanie zásad SLP v testovacom pracovisku.

Pred každým výberom musí byť k dispozícii podrobný opis očakávaní od používania cloudového riešenia a súvisiacich vplyvov. Kroky hodnotenia rizík zahŕňajú (okrem iného):

1. Očakávané ciele a funkcie vrátane systémových požiadaviek, požiadaviek používateľov a obmedzení pre systém.
2. Infraštruktúra a aplikácie: rozsah, v akom sa očakáva poskytovanie infraštruktúry, siete/platforiem a aplikácií.
3. Vplyv na dodržiavanie súladu so zásadami SLP, najmä pokiaľ ide o migráciu a ukladanie údajov, vyplývajúci z prijatia systému, poskytovaného cloudovou službou (neúplný zoznam):

a. Očakávaný nový proces spracovania údajov a zmeny oproti súčasnému systému: predovšetkým by sa mali dôkladne identifikovať a opísať kroky na migráciu dát.

b. Súvisiace nové riziká týkajúce sa kvality údajov: riziká spojené s novo dodávanými aplikáciami na zachytávanie, generovanie alebo analýzu údajov (spoľahlivosť, dostupnosť systému a údajov, plány zálohovania pre prípad zlyhanie systému).

c. Súvisiace nové riziká týkajúce sa integrity údajov a dostupnosti údajov: úroveň kontroly vzdialeného prístupu k údajom, úroveň ochrany údajov, bezpečné miesto pre fyzické uloženie údajov (fyzický prístup k infraštruktúre, stratégia obnovy po havárii, ciele týkajúce sa času obnovy a bodov obnovy, umiestnenie serverov, na ktorých sú údaje umiestnené, dlhodobá integrita elektronicky archivovaných údajov). V prípade SaaS, keďže testovacie pracovisko vo všeobecnosti nemá prístup k samotnému softvéru v prípade jeho uvoľnenia do používania, koncový používateľ by mal dôkladne zvážiť vplyv na integritu údajov a dostupnosť údajov pri predvídaní plánu kontinuity podnikania, plánu obnovy po havárii a stratégiu odchodu testovacieho pracoviska SLP od dodávateľa SaaS.

d. Dopady na systémovú architektúru (tak systémovú architektúru testovacieho pracoviska, aj systémovú architektúru poskytovateľa cloudových služieb), organizáciu a model prevádzky.

e. Dopady na ochranu vlastníctva údajov.

f. Dopady na kompetencie personálu štúdie, vedúcich štúdií, pracovníkov zabezpečovania kvality a archivára, najmä potreba ich školení.

4. Očakávané opatrenia na zmiernenie zistených rizík vrátane (neúplný zoznam):

   a. Potreba primeraných kontrol na udržanie alebo overenie kvality údajov, integrity údajov a dostupnosti údajov a potreba preskúmania údajov.

   b. Tam, kde je to vhodné, existencia auditných záznamov (audit trails).

5. Stanovené kritériá pre výber poskytovateľa cloudových služieb vrátane dodržiavania špecifických noriem kvality a dostupnosti pohotovostných plánov pre prípad zlyhania poskytovateľa, ako je obnova po havárii, bezpečnosť poskytovateľa cloudových služieb atď. (pozri tiež kap. 5.5.3.2 „Hodnotenie poskytovateľa cloudových služieb“).

6. Plán migrácie služby v prípade ukončenia poskytovania služby poskytovateľom.

7. Archivácia (v prípade potreby).

Pri výbere cloudového riešenia sa musí vytvoriť jasný a úplný opis a plán implementácie. Ten by mal zahŕňať:

1. Poskytovateľa(-ov) cloudových služieb: názov (-y) a adresu (-y) spoločnosti (ak sú známe, adresy dátových centier) a kontakty, odkaz na zmluvu (-y).

2. Podrobnosti o všetkých subdodávateľoch poskytovateľa (-ov) cloudových služieb relevantných z hľadiska dodržiavania SLP: technická úloha, názvy a adresy, odkaz na zmluvy.

3. Prehľad zvoleného riešenia s podrobným opisom, nedostatkami medzi očakávanými a poskytovanými funkciami, vybrané služby/produkty, zúčastnené strany a miesto(-a) dodania.

4. Podrobná špecifikácia činností vykonávaných poskytovateľom cloudových služieb (pozri tabuľku 1.), najmä rozdelenie technických úloh, rolí a zodpovedností medzi poskytovateľom cloudových služieb, jeho subdodávateľmi a testovacím pracoviskom (pozri kap. 5.5.3.3 „Dohoda o úrovni služieb / Service Level Agreement (SLA)“) .
5. Podrobný proces validácie vrátane úloh a prostriedkov, ktoré poskytuje poskytovateľ cloudových služieb (vrátane možného prístupu, ak je to relevantné, k testovaciemu prostrediu, v ktorom sa systém môže testovať pred uvedením do prevádzky).
6. Podrobná špecifikácia zabezpečujúca kontrolu prístupu k údajom (vzdialený prístup, prístup poskytovateľov cloudových služieb k systémom a údajom, prístup poskytovateľov cloudových služieb k vykonávaniu zmien priamo v databáze tam, kde je to vhodné), úroveň ochrany údajov (vrátane činností v oblasti bezpečnosti IT, napr. správa a kontrola prístupov používateľov, správa hesiel, správa firewallov, zálohovanie a obnova, riešenie bezpečnostných incidentov, údržba a bezpečnostné záplaty platforiem (databáz a operačných systémov), detekcia a ochrana proti vniknutiu.
7. Určenie typu modelu služby, ktorý sa má implementovať – IaaS, PaaS alebo SaaS.
8. Určenie typu modelu nasadenia – súkromný, verejný, komunitný alebo hybridný.
9. ŠPP potrebné na riadenie bežného používania, správy a údržby systému.
10. Školenie personálu testovacieho pracoviska, ak je to potrebné.
11. Prostriedky kontroly cloudového riešenia testovacím pracoviskom: tieto kontroly sa musia naplánovať tak, aby sa overilo, že je systém udržiavaný vo validovanom stave, aby sa zabezpečila kvalita údajov, integrita údajov a ich dostupnosť. Tieto audity sa musia vykonávať nezávisle od poskytovateľa cloudových služieb (interného alebo externého poskytovateľa), musia byť monitorované a dokumentácia sa musí uchovávať. Úsilie o kontrolu by malo byť spojené s funkciami, ktoré zabezpečuje cloudové riešenie. Napríklad:
    a. Ak sa cloudové riešenie používa na archiváciu údajov, musia sa zaviesť pravidelné kontroly na overenie integrity údajov a dostupnosti údajov v archívoch. Frekvencia takýchto kontrol musí byť založená na riziku.
    b. Ak je cloudové riešenie SaaS, kvalitu údajov, integritu údajov a dostupnosť údajov je možné overiť elektronickými kontrolami pri každom spustení alebo periodicky, kontrolnými súčtami, preskúmaním záznamov auditu alebo prístupov alebo akýmikoľvek inými riešeniami. Frekvencia takýchto kontrol musí byť založená na riziku. Pravidelné správy o aplikácií SaaS, ktoré môže poskytovať poskytovateľ cloudových služieb, nemôžu nahradiť nezávislé kontroly.

5.5.3.2. Hodnotenie poskytovateľa cloudových služieb

Poznámka: Manažment poskytovateľa cloudových služieb zohráva dôležitú úlohu pri zabezpečovaní kvality a súladu služieb. Požiadavky testovacieho pracoviska na poskytovateľa cloudových služieb na zabezpečenie úrovne služieb, ktorá je vhodná na účely použitia SLP, musia byť definované v dohode o úrovni služieb (pozri kap. 5.5.3.3.„Dohoda o úrovni služieb / Service Level Agreement (SLA)“).

Stanovené kritériá na výber poskytovateľov cloudových služieb musia byť zdokumentované.

Kompetentnosť a spoľahlivosť poskytovateľa cloudových služieb sú kľúčovými faktormi pri výbere produktu alebo poskytovateľa služby. Môže byť vhodné vykonať audit poskytovateľa cloudových služieb a rozhodnutie o vykonaní alebo nevykonaní auditu u poskytovateľa cloudových služieb musí byť založené na zdokumentovanom posúdení rizika. Súčasťou audítorského tímu by mali byť aj používatelia, pracovníci QA, odborníci na IT a/alebo externí odborníci.

Činnosti poskytovateľov cloudových služieb môžu byť subdodávateľsky zadané iným dodávateľom. V prípade akejkoľvek subdodávky je konečnou zodpovednosťou testovacieho pracoviska posúdiť a preukázať, že cloudové služby neovplyvňujú súlad testovacieho pracoviska so zásadami SLP.

Pri hodnotení poskytovateľa cloudových služieb je nevyhnutné overiť, aký (ak vôbec nejaký) systém kvality je zavedený u poskytovateľa cloudových služieb (vrátane systémov príslušných subdodávateľov).

Poskytovateľ cloudových služieb (a subdodávateľ) môže mať certifikované systémy kvality. Testovacie pracovisko ich môže vziať do úvahy, ak podporujú súlad testovacieho pracoviska so zásadami SLP.

> **Poznámka:** Niektoré národné predpisy (iné ako SLP) môžu vyžadovať, aby poskytovatelia cloudových služieb mali definované certifikáty o úrovni bezpečnosti, ktoré poskytujú pred zabezpečením hosťovania niektorých špecifických údajov (napr. osobné údaje, lekárske údaje, zdravotné údaje). Zodpovednosť TFM sa obmedzuje na otázky dodržiavania zásad SLP.

Testovacie pracovisko sa môže tiež rozhodnúť zadať posúdenie poskytovateľa cloudových služieb externému odborníkovi. Vhodnosť tohto postupu musí posúdiť TFM s podporou QA.

Počas posudzovania sa môžu riešiť nasledujúce všeobecné body (neúplný zoznam):

1. Systém kvality poskytovateľa cloudových služieb, ak existuje (vrátane subdodávateľa(ov) a riadenia štandardných pracovných postupov).
2. Proces dokumentácie.
3. Personálny manažment (vrátane školení).
4. Dôvernosť a bezpečnosť.
5. Kontrola prístupu k údajom.
6. Priestory a používaná technológia.
7. Kvalifikácia zariadení zapojených do systému v rozsahu pôsobnosti.
8. Kvalifikácia systému v rozsahu pôsobnosti (overenie, či sú požadované funkcionality úspešne otestované).
9. Pochopenie a politika integrity údajov.
10. Zálohovanie a testy obnovy.
11. Procesy obnovy po havárii.
12. Stratégia odchodu.
13. Zdroje technickej pomoci

Pokiaľ ide o samotné cloudové riešenie a súvisiace služby, testovacie pracovisko musí posúdiť, či poskytovanie cloudových služieb spĺňa vopred definované požiadavky. Poskytovateľ cloudových služieb musí mať ľahko dostupné systémy a informácie, ktoré sú primerané činnostiam, ktoré vykonáva, aby podporil súlad so zásadami SLP. Poskytovatelia cloudových služieb musia mať (s ohľadom na služby, ktoré poskytujú):

1. Osobné záznamy všetkých zamestnancov priamo zapojených do služieb poskytovaných testovaciemu pracovisku vrátane:
    1. Záznamov o vzdelaní/príprave a odbornej praxi.
    2. Záznamov o ďalšom vzdelávaní v oblasti IT a riadenia kvality, ktoré sú potrebné na plnenie ich povinností.
    3. Opis súčasných povinností a úloh (napr. opis práce, organizačná schéma).
2. Školenie zamerané na zvyšovanie povedomia o SLP. Môže ísť o stratégiu TFM na zmiernenie rizika, s cieľom zabezpečiť, aby kľúčoví pracovníci rozumeli predpisom a požiadavkám SLP, ktoré sa vzťahujú na poskytované služby, najmä pokiaľ ide o bezpečnosť a uchovávanie údajov.
3. Osobitné ustanovenia týkajúce sa cloudových služieb vrátane napríklad:
    a. Dokumentácia o životnom cykle poskytovaného systému.
    b. Integrita údajov, pochopenie dátových tokov, spracovanie údajov.
    c. Zálohovanie a obnova elektronických údajov a záznamov.
    d. Archivácia elektronických údajov a záznamov.
    e. Vlastníctvo elektronických údajov a prístupové práva.
    f. Riadenie zmien a uvoľňovania.
    g. Riadenie subdodávateľov, ak je to vhodné.
4. Dokumentáciu o všetkých činnostiach vykonávaných v mene testovacieho pracoviska, ktorá zabezpečuje vysledovateľnosť týchto činností.
5. Poskytnutý prístup k dokumentom, podľa požiadaviek pri inšpekciách alebo auditoch zabezpečenia kvality.
6. Mať k dispozícii adekvátne validované vybavenie/hardvér.

Testovacie pracovisko musí overiť, či sú dokumentácia a postupy poskytovateľa cloudových služieb primerané na zabezpečenie vhodného kvalifikačného a validačného prístupu k poskytovaným službám.

5.5.3.3. Dohoda o úrovni služieb / Service Level Agreement (SLA)

> **Poznámka:** Na označenie dokumentov, v ktorých sú opísané prevádzkové ustanovenia pre cloudovú službu, sa používajú rôzne výrazy: zmluvy, dohody o zabezpečení kvality, technické špecifikácie atď. V tomto dokumente sa používa pojem Dohoda o úrovni služieb (Service Level Agreement SLA).

Posúdenie rizík, validácia systému, hodnotenie poskytovateľa cloudových služieb a dohoda o úrovni služieb musia jasne uvádzať, že pri implementácii cloud computingu v testovacom pracovisku sú pokryté príslušné aspekty týkajúce sa kvality údajov, integrity údajov a dostupnosti údajov. Medzi testovacím pracoviskom SLP a poskytovateľmi cloudových služieb musia

existovať formálne dohody - zmluvy. Tieto zmluvy musia obsahovať jasné povinnosti subdodávateľov poskytovateľov cloudových služieb s uvedením zodpovednosti za údaje všetkých tretích strán, ktoré sa podieľajú na službe.

SLA je ústredným dokumentom, ktorý definuje všetky aspekty spolupráce medzi testovacím pracoviskom SLP a poskytovateľom cloudových služieb. Zmluva SLA sa musí zaoberať všetkými relevantnými aspektami vrátane, ale nie výlučne, zodpovedností, využívania subdodávateľov, dokumentácie, výkonu, archivácie, školenia, komunikácie, spôsobu hlásení, auditov, validácie.

Využitie subdodávateľov poskytovateľom cloudových služieb nemôže ovplyvniť kvalitu údajov, integritu údajov a dostupnosť údajov ani celkový súlad so zásadami SLP v testovacom pracovisku. Musia byť zavedené vhodné opatrenia na riadny prevod činnosti, údajov alebo služieb od dodávateľa k subdodávateľovi. Využívanie subdodávateľov musí byť vopred povolené v zmluve medzi testovacím pracoviskom a poskytovateľom cloudových služieb.

Hoci neexistuje žiadna všeobecná požiadavka, aby dodávateľ sám spĺňal požiadavky zásad SLP, všetky požiadavky relevantné na zabezpečenie kvality údajov, integrity údajov a dostupnosti údajov musia byť zahrnuté v SLA. SLA by mala umožniť poskytovateľovi cloudových služieb pochopiť a prevziať svoje povinnosti týkajúce sa údajov aj tých, ktoré sú zverené jeho subdodávateľovi (-om). Testovacie pracovisko má vykonať náležité procesy na zabezpečenie toho, že poskytovaná služba neohrozí integritu údajov a vo všeobecnosti podporuje dodržiavanie súladu so zásadami SLP.

Úlohy a zodpovednosti

Úlohy a zodpovednosti testovacieho pracoviska a poskytovateľa cloudových služieb musia byť jasne opísané.

TFM nesie celkovú zodpovednosť za súlad so zásadami SLP počas celého životného cyklu svojich počítačových systémov a za podporné služby IT, aj keď tieto služby poskytujú poskytovatelia cloudových služieb.

Poskytovateľ cloudových služieb je zodpovedný za poskytnutie cloudových služieb, ktoré umožňujú testovaciemu pracovisku splniť všetky príslušné požiadavky zásad SLP, ako je uvedené v SLA.

Ak sú činnosti poskytovateľa cloudových služieb zadané iným dodávateľom (subdodávka) je potrebné sa týmto zaoberať. V SLA musí byť uvedený zoznam subdodávateľov, subdodávaných činností a súvisiacich zodpovedností.

Odporúča sa, aby QA skontrolovala návrh SLA, s cieľom zabezpečiť splnenie všetkých aspektov súladu so zásadami SLP, avšak konečná zodpovednosť za schválenie SLA zostáva na TFM.

V SLA sa musia definovať spôsoby pravidelného preskúmania existujúcich SLA. Možnosť auditov poskytovateľa cloudových služieb musí byť definovaná v SLA a naplánovaná v pláne QA testovacieho pracoviska.

Dokumentácia, ako sú ŠPP, personálne záznamy, správy, dokumentácia kontroly zmien oboch strán, musí obsahovať príslušné informácie z SLA. Každá strana musí udržiavať dokumentáciu vyžadovanú SLA.

Životný cyklus systému

V SLA musia byť opísané povinnosti poskytovateľa cloudových služieb (a prípadného subdodávateľa (-ov)) a testovacieho pracoviska počas životného cyklu podporovaných systémov. To zahŕňa inštaláciu, konfiguráciu, integráciu, validáciu, údržbu (napr. prostredníctvom vzdialeného prístupu), úpravu, uchovanie alebo vyradenie systému. Minimálne je potrebné zahrnúť tieto body:

1. Ukladanie údajov.
2. Bezpečnosť.
3. Kontrola zmien (vrátane aktualizácií aplikácií/softvéru) a správa konfigurácie. S poskytovateľom cloudových služieb je potrebné prediskutovať časové obdobie, ktoré musí byť definované v SLA, aby testovacie pracovisko mohlo vykonať testovanie pred implementáciou zmien v cloudových službách. V SLA sa tiež má uviesť, že testovaciemu pracovisku budú poskytnuté podrobnosti o úpravách novej verzie a dokumentácia o validácii. V prípade potreby musí byť k dispozícii prístup k testovaciemu prostrediu, v ktorom je možné testovať novú verziu systému pred jeho uvedením do prevádzky.
4. Riadenie incidentov.
5. Kontinuita prevádzky (vrátane zálohovania a obnovy, najmä intervaly zálohovania, podrobnosti o možných miestach zrkadlenia, očakávané zdokumentované potvrdenia o zálohovaní a zrkadlení, čas na obnovenie atď.).
6. Kvalifikovaná infraštruktúra.
7. Správa údajov.
8. Integrita údajov zachovaná počas obdobia uchovávania záznamov.
9. Periodické hodnotenie testovacím pracoviskom.

Bezpečnosť a kontrola prístupu

Vhodné technické a organizačné opatrenia zabezpečia logickú a fyzickú bezpečnosť a dostupnosť údajov aj systémov. Údržba systémov a riadenie incidentov musia byť opísané v SLA.

SLA sa musí týkať aj riadenia prístupových oprávnení, vrátane pravidelného preskúmania prístupov, pričom tie by mali byť obmedzené na oprávnených pracovníkov bez ohľadu na spôsob prístupu do systému.

V SLA má byť uvedené, že poskytovateľ cloudových služieb alebo jeho subdodávateľ nemajú mať prístup k údajom, migrovať ich (manuálne, nie prostredníctvom správcu úložiska), meniť, upravovať alebo odstraňovať bez predchádzajúceho písomného povolenia od TFM.

Musia sa definovať postupy, ako zabrániť kybernetickým útokom, vrátane, ale nie výlučne, prístupu k elektronickým údajom počas útokov a ako obnoviť údaje a zabezpečiť integritu nespracovaných údajov, po ich opätovnom sprístupnení.

Dokumentácia poskytovateľa cloudových služieb o systémoch

SLA musí definovať, ktoré záznamy sa majú uchovávať a archivovať. Ďalej musí definovať fyzické a/alebo logické miesto archivácie a dobu uchovávania. Testovacie pracovisko musí definovať dokumenty a záznamy poskytovateľa cloudových služieb, ktoré zabezpečujú požadovanú sledovateľnosť poskytovaného systému a overiť dostupnosť takejto dokumentácie. Všetky definované dokumenty musia byť prístupné testovaciemu pracovisku a inšpektorom orgánov monitorujúcich dodržiavanie zásad SLP.

Komunikácia

Komunikačné linky medzi testovacím pracoviskom a poskytovateľom cloudových služieb musia byť opísané v SLA. Je potrebné definovať komunikačné prostriedky, ako sú fyzické alebo virtuálne stretnutia, telefón, e-mail alebo horúca linka. Musí existovať dohoda o tom, ktoré informácie sa majú zdieľať (riadenie incidentov, kontrola zmien, prístup dodávateľa k údajom atď.). Obe strany musia spolupracovať, aby zabezpečili vyhovujúcu a správnu prevádzku systému a udržali kvalifikovaný a validovaný stav systému.

Stratégia odchodu

V SLA musí byť jasne opísané právo testovacieho pracoviska na získanie všetkých údajov a metaúdajov (vrátane auditných záznamov) v čitateľnom a konvertibilnom formáte v prípade ukončenia zmluvy s poskytovateľom cloudových služieb (pozri tiež dokument OECD Guideline No. 22 kapitola 6).

Konečná likvidácia údajov

V SLA musí byť definovaný proces likvidácie údajov po ukončení zmluvy. V SLA sa musí uvádzať, že poskytovateľ cloudových služieb po ukončení platnosti zmluvy o poskytovaní služieb efektívne a nezvratne odstráni a zničí všetky zálohované údaje (určené na obnovenie po havárii) patriace testovaciemu pracovisku. Poskytovateľ cloudových služieb musí na žiadosť testovacieho pracoviska poskytnúť dokument o takomto odstránení a zničení.

5.5.3.4. Validácia počítačových systémov v cloudovej službe

Podmienkou používania počítačových systémov v SLP je, že testovacie pracovisko musí používať iba validované systémy, bez ohľadu na to, či ide o SaaS alebo sú hosťované na IaaS/PaaS.

Musia byť splnené všetky požiadavky týkajúce sa validácie počítačového systému. Rozhodnutia o rozsahu validačných činností a kontrol integrity údajov, ktoré sa vykonávajú v rámci zodpovednosti TFM, musia vychádzať z odôvodneného a zdokumentovaného hodnotenia rizika počítačového systému.

Testovacie pracovisko zabezpečí, aby boli všetky počítačové systémy riadne validované. Testovacie pracovisko jasne zadefinuje špecifikácie požiadaviek používateľa. (aj keď môžu pochádzať z validačnej dokumentácie poskytovateľa cloudových služieb).

Testovacie pracovisko musí rozumieť, čo je potrebné validovať (aplikáciu ako vhodnú na jej zamýšľané použitie v rámci procesu), kto je zodpovedný za zabezpečenie splnenia všetkých požiadaviek na validáciu počítačového systému.

Ak časť validačnej dokumentácie dodáva poskytovateľ cloudových služieb, testovacie pracovisko posúdi jej relevantnosť v procese validácie. V prípade, že sa používa validačná dokumentácia od poskytovateľa cloudových služieb, musí byť čitateľne dostupná v testovacom pracovisku.

Napríklad v prípade SaaS:

1. Poskytovateľ cloudových služieb poskytne dôkaz o tom, že bola vykonaná úspešná inštalácia a správa aplikácie, ako je napríklad funkčné testovanie aplikácie, automatizované testovanie, testovanie jednotiek, testovanie aplikačného programovacieho rozhrania (API); aj keď sa to mohlo uskutočniť nezávisle od zapojenia testovacieho pracoviska. Poskytovateľ cloudových služieb môže kvalifikovať hostingové infraštruktúry. ŠPP pre životný cyklus aplikácie spravidla vydáva poskytovateľ cloudových služieb. TFM posúdi prácu poskytovateľa cloudových služieb, aby sa potvrdilo, že bola vykonaná správne pre systém používaný v testovacom pracovisku a aby sa zistilo, čo chýba. TFM zdokumentuje a schváli toto posúdenie.
2. Testovacie pracovisko vykoná všetky dodatočné testy, ktoré je potrebné dokončiť, najmä testovanie v prostredí testovacieho pracoviska a kontroly potrebné na trvale vyhovujúce používanie systému (vrátane školenia používateľov, vydania ŠPP na používanie aplikácie v prostredí SLP).

Rovnako ako v prípade všetkých počítačových systémov, testovacie pracovisko musí prijať náležité opatrenia a mať zavedené postupy pre prípad, že sa skončí dohoda s poskytovateľom cloudových služieb alebo bude jeho systém vyradený z prevádzky, aby sa zabezpečilo, že všetky údaje a metadáta (vrátane všetkých auditných záznamov), ktoré je potrebné na predpísanú dobu uchovať, budú vhodným spôsobom archivované alebo presunuté. Ustanovenia o stratégii ukončenia na zabezpečenie obnovy údajov by sa mali podľa možnosti otestovať počas validácie systému.

5.6 POŽIADAVKY ORGÁNOV MONITORUJÚCICH DODRŽIAVANIE SLP PRI KONTROLE CLOUDOVÝCH RIEŠENÍ

Systémy SLP musia byť validované a prevádzkované spôsobom, ktorý zabezpečí výsledok a integritu údajov SLP bez ohľadu na to, či sú nainštalované lokálne alebo poskytované ako cloudová služba.

5.6.1 Implementácia cloudového riešenia

Na umožnenie overenia cloudových služieb inšpektormi SLP musí byť k dispozícii nasledujúca dokumentácia:

1. Záznamy o implementovaných systémoch vrátane zdôvodnenia výberu systémov, posúdenia rizík týkajúcich sa kvality a integrity údajov a opisu implementovaných systémov.
2. Dokumentácia o procese validácie:
    a. V testovacom pracovisku musí byť k dispozícii dokumentácia o kvalifikačných činnostiach, ktoré vykonáva poskytovateľ cloudových služieb.
    b. Počas inšpekcie musí byť poskytnutý dôkaz o tom, (buď samotným testovacím pracoviskom alebo s pomocou poskytovateľa cloudových služieb,

ak sa testovacie pracovisko čiastočne spolieha na kvalifikačnú dokumentáciu poskytnutú dodávateľom), že kvalifikačné činnosti poskytované cloudovou službou boli vyhodnotené ako úplné a primerané.

c. K dispozícii musí byť aj dokumentácia dodatočných kvalifikačných/validačných činností založených na zdokumentovanom hodnotení rizika, ktoré vykonáva testovacie pracovisko.

3. Zdôvodnenie výberu poskytovateľa cloudových služieb (pozri tiež časť „Posúdenie poskytovateľa cloudových služieb“), aj keď interné, musí byť k dispozícii a musí zahŕňať zdokumentované hodnotenie/audit systému kvality poskytovateľa cloudových služieb a procesov kvalifikácie a validácie. Testovacie pracovisko musí adekvátne znížiť dopad všetkých zistených nedostatkov.
4. Dohoda o úrovni služieb medzi testovacím pracoviskom a poskytovateľom cloudových služieb s jasným opisom spoločných činností a zodpovedností v systéme.

5.6.2 Životný cyklus aplikácie cloudovej služby

K dispozícii musia byť dôkazy o opatreniach implementovaných testovacím pracoviskom na zabezpečenie nepretržitej platnosti cloudového riešenia (samotným testovacím pracoviskom alebo vyžiadané prostredníctvom SLA s poskytovateľom cloudových služieb). To zahŕňa ustanovenia na zabezpečenie (neúplný zoznam):

1. Dostupnosť, údržba, aktualizácie, kontinuita prevádzky, plán obnovy po havárii a plán migrácie systému.
2. Integrita údajov počas celého životného cyklu.
3. Kvalita údajov počas celého životného cyklu.
4. Dostupnosť údajov.
5. Nezávislý plán kontrol implementovaný a vykonávaný testovacím pracoviskom, aby sa zabezpečilo, že cloudový systém zostane počas svojho životného cyklu vo validovanom stave.
6. Dokumentácia o vzdialenom prístupe a autentifikácii.
7. Stratégia ukončenia zmluvy musí po skončení zmluvy jasne opisovať, ako testovacie pracovisko získa všetky údaje a metaúdaje (vrátane auditných záznamov) v čitateľnom a konvertibilnom formáte v prípade, že dôjde k ukončeniu zmluvy s poskytovateľom cloudových služieb.

Okrem dokumentácie môžu inšpektori požadovať aj demonštráciu fungovania systému, aby overili jeho súlad. Testovacie pracovisko musí mať pre inšpektorov k dispozícii podrobnosti o funkčných skúškach systému.

5.6.3 Elektronické archívy v cloudovom riešení

Poskytovatelia cloudových služieb môžu pôsobiť ako zmluvný archív poskytovaním služieb alebo komponentov na uchovávanie a archivovanie relevantných SLP údajov a záznamov.

Orgány monitorujúce dodržiavanie SLP majú rôzne prístupy k zmluvným archívom. Niektorí ich zaraďujú do svojich monitorovacích programov ako poskytovateľov archívov SLP; iní ich berú

do úvahy pri inšpekcii testovacieho pracoviska. Elektronické archívy musia byť v súlade s platnými zásadami SLP (vrátane dokumentu OECD Guideline No. 15) a TFM musí v konečnom dôsledku zabezpečiť, aby sa tak stalo. Monitorovacie orgány môžu tiež kontrolovať dodržiavanie SLP poskytovateľov cloudových služieb.

Inšpekcia umiestnenia serverov používaných na archiváciu (napr. budov, miestností a skríň) s cieľom overiť fyzickú bezpečnosť hostiteľských zariadení nie je vždy možná, najmä ak je umiestnenie neznáme. Treba však poznamenať, že niektoré orgány monitorujúce dodržiavanie SLP vyžadujú podrobnosti o umiestnení cloudového archívu na fyzické overenie, čo vylučuje použitie serverov s neznámou polohou na hosťovanie elektronických archívov.

Testovacie pracovisko musí byť schopné poskytnúť zdokumentované dôkazy o súlade so zásadami SLP pre archív, ako je dohoda o úrovni služieb a hodnotenie/audit poskytovateľa cloudových služieb aj systému.

Musia byť k dispozícii informácie o počítačových systémoch a poskytovateľoch cloudových služieb, ktoré podporujú logickú a technickú integritu. To by zahŕňalo dôkazy o úplnej kontrole zo strany archivára, kontrolu prístupu, inventár pre indexované riadne uloženie, možnosť obnovenia záznamu, dôkaz integrity záznamu a sledovateľnosť od prvotných údajov až po konečnú správu.

Relevantnosť všetkých opatrení na zabezpečenie logickej, technickej a fyzickej integrity je potrebné zdokumentovať v odôvodnení založenom na hodnotení rizika.

Dôležité sú opatrenia, ako je politika zálohovania založená na hodnotení rizika. Musí byť dostupný zdokumentovaný dôkaz o relevantných a účinných opatreniach zálohovania a zrkadlenia a protokoloch obnovy a kontrole týchto procesov zo strany testovacieho pracoviska.

5.7 ZÁVER

Poskytovatelia cloudových služieb môžu ponúkať rôzne riešenia, ktoré umožňujú získavanie údajov pre bezpečnosť ľudí, zvierat a životného prostredia. Implementácia cloudového riešenia nemôže ohroziť súlad činností SLP, musí byť zaručená kvalita, integrita a dostupnosť údajov.

Pri vykonávaní inšpekcie s cloudovými službami zapojenými do procesov testovacieho pracoviska inšpektori SLP očakávajú, že TFM bude schopný preukázať, že implementovaná cloudová služba stále zabezpečuje súlad so zásadami SLP a že TFM má primerané prostriedky na jej kontrolu.

5.8 SLOVNÍK

Zálohovanie / **Back-up:** (pozri OECD Guideline No. 17 resp. MSA-G/17).

Kontrola zmeny /Change control: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Počítačový systém / Computerised system: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Údaje / Data: (pozri OECD Guideline No. 17 a No. 22 resp. MSA-G/17 a MSA-G/22).

Databáza / Database: Databáza je informácia, ktorá je nastavená na jednoduchý prístup, správu a aktualizáciu. Počítačová databáza je organizovaná zbierka údajov uložených, udržiavaných a prístupných elektronicky. Malé databázy môžu byť uložené v súborovom systéme, zatiaľ čo veľké databázy sú hosťované v počítačových klastroch alebo cloudových úložiskách.

Dátové centrum /Data centre: Dátové centrum je fyzické zariadenie, ktoré sa používa na umiestnenie elektronických aplikácií a údajov. Dizajn dátového centra je založený na sieti výpočtových a úložných zdrojov, ktoré umožňujú poskytovanie zdieľaných aplikácií a údajov. Medzi kľúčové komponenty dizajnu dátového úložiska patria smerovače, prepínače, firewally, úložné systémy, servery a kontroléry doručovania aplikácií.

Ochrana údajov / Data protection: Ochrana údajov je proces ochrany údajov pred poškodením, kompromitáciou alebo stratou a poskytuje možnosť obnoviť údaje do funkčného stavu, keď sa stane niečo, čo spôsobí, že údaje budú nedostupné alebo nepoužiteľné.

Šifrovanie / Encryption: Šifrovanie údajov konvertuje údaje z čitateľného formátu obyčajného textu do nečitateľného zakódovaného formátu. Používatelia a procesy môžu čítať a spracovávať zašifrované údaje až po ich dešifrovaní. Dešifrovací kľúč je tajný a chránený pred neoprávneným prístupom.

Hardvér /Hardware: Hardvér označuje hmatateľné komponenty počítača alebo doručovacie systémy, ktoré uchovávajú a spúšťajú písomné pokyny poskytnuté softvérom.

Kvalifikácia / Qualification: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Kvalifikovaná/overená infraštruktúra / Qualified/verified infrastructure: Kvalifikácia IT infraštruktúry je proces preukázania, že IT komponenty sú vyvinuté tak, aby boli vhodné na ich zamýšľané použitie, spĺňali špecifikované požiadavky a že stav vhodnosti systému je udržiavaný počas každého bodu životného cyklu systému.

Životný cyklus / Life cycle: (pozri OECD Guideline No. 17 /pre životný cyklus počítačového systému/ a No. 22 /pre životný cyklus údajov/ resp. MSA-G/17 a MSA-G/22).

Sieť / Network: Počítačová sieť je súbor počítačov, ktoré zdieľajú zdroje umiestnené na sieťových uzloch alebo poskytované sieťovými uzlami. Počítače používajú na vzájomnú komunikáciu bežné komunikačné protokoly cez digitálne prepojenia.

Operačný systém / Operating system: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Ciele doby obnovy / Recovery time objectives: Cieľ doby obnovy je cieľ, ktorý si organizácia stanoví na maximálnu dĺžku času, ktorú by mala trvať obnova normálnych operácií po výpadku alebo strate údajov.

Ciele obnovy stavu údajov /Recovery point objectives: Ako cieľ obnovy stavu si organizácia stanoví maximálne množstvo údajov, ktorých stratu ešte môže tolerovať. Tento parameter sa meria časom: od okamihu, keď dôjde k zlyhaniu až po poslednú platnú zálohu údajov pred výpadkom.

Riziko / Risk: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Hodnotenie rizika / Risk assessment: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Zmiernenie rizika / Risk mitigation: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Zabezpečenie / Security: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Server / Server: Server je softvérové alebo hardvérové zariadenie, ktoré prijíma a odpovedá na požiadavky uskutočnené cez sieť. Zariadenie, ktoré zadáva požiadavku a prijíma odpoveď zo servera, sa nazýva klient.

Softvér / Software: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Validácia / Validation: (pozri OECD Guideline No. 17 resp. MSA-G/17).

Virtuálna súkromná sieť (VPN) / Virtual Private Network (VPN): Virtuálna súkromná sieť alebo VPN je šifrované pripojenie cez internet zo zariadenia do siete alebo medzi dvoma sieťami. Šifrované spojenie zaisťuje bezpečný prenos citlivých údajov. Zabraňuje neoprávneným osobám odpočúvať komunikáciu a umožňuje užívateľovi vykonávať prácu na diaľku.

***