

Technická a funkčná špecifikácia

Príloha č. 1/A – Opis predmetu zákazky

Cieľom modulu Pravidlá a požiadavky týkajúce sa výrobkov je vytvorenie databázového systému, ktorý bude obsahovať pravidlá a požiadavky týkajúce sa výrobkov (vnútroštátne právne predpisy) platné v Slovenskej republike, v harmonizovanej aj neharmonizovanej oblasti, ktorý umožní

1. interný manažment údajov,
2. dynamickú tvorbu a prepájanie číselníkov,
3. manažment prístupov organizácií k manažmentu dát, ktoré podliehajú ich gescii,
4. vyhľadávanie a filtrovanie dát pre externého používateľa s požadovanými výstupmi,
5. prepojenie na dátovú časť Centrálného repozitára noriem,
6. api pre publikovanie vybraných číselníkov a dát pre data.gov.sk,
7. api interface pre komunikáciu s modulom M3.

Číselníky

Aplikácia bude obsahovať nasledujúce základné číselníky:

1. Zoznam organizácií
2. Druh výrobku
3. Kategória vnútroštátneho predpisu
4. Autorizované a notifikované osoby
5. Ukončenie posudzovania zhody
6. Vnútroštátne predpisy
7. Harmonizované predpisy
8. Neharmonizovaná oblasť, všeobecné predpisy
9. Neharmonizovaná oblasť, špecifické predpisy
10. Príklady výrobkov
11. Druh osvedčenia o akreditácii
12. Skupina výrobkov

1. **Zoznam organizácií** – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
slovenská skratka organizácie	String (20)	Áno
slovenský názov organizácie	String (255)	Áno
sekcia/odbor/oddelenie danej organizácie	String (255)	Nie
anglický názov organizácie	String (255)	Nie
kontaktná e-mailová adresa organizácie	String (255)	Nie
url kontakt pre sk verziu	String (255)	Nie

url kontakt pre en verziu	String (255)	Nie
prepojenie/vzťah na nadriadenú organizáciu	(vzťah)	Nie

2. Druh výrobku – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
druh výrobku v sk	String (255)	Áno
druh výrobku v en	String (255)	Nie
kód podľa colného sadzovníka	String (255)	Nie

3. Kategória vnútroštátneho predpisu– atribúty vystupujúce v entite

Názov	Typ	Povinné pole
kategória vnútroštátneho predpisu v sk	String (255)	Áno
kategória vnútroštátneho predpisu v en	String (255)	Nie

4. Autorizované a notifikované osoby – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
identifikačný kód autorizovanej osoby	String (10)	Áno
url autorizovanej osoby	String (255)	Nie
názov spoločnosti autorizovanej osoby	String (255)	Áno
url spoločnosti autorizovanej osoby	String (255)	Nie
číslo notifikovanej osoby	String (5)	Nie
url odkaz na notifikovanú osobu 1 (odkaz na NANDO pre konkrétnu NO)	String (255)	Nie

url odkaz na notifikovanú osobu 2 (odkaz na NANDO pre všetky/ostatné NO)	String (255)	Nie
vzťah/prepojenie na druh výrobku (môže ich byť viac)	(vzťah)	
postup posudzovania zhody (url odkaz)		
vzťah na skupinu výrobkov (môže ich byť viac)	(vzťah)	Nie
prepojenie na harmonizované predpisy	(vzťah)	Nie
postupy posudzovania zhody (moduly)		
príloha č.	String (255)	Nie
akreditácia/granted accreditation	String (255)	Nie
EA-2/17 Systém		
číslo osvedčenia o akreditácii	Prepojenie na druh osvedčenia	
koniec platnosti osvedčenia	date	

5. Ukončenie posudzovania zhody – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
názov zhody v sk	String (255)	Áno
názov zhody v en	String (255)	Nie
možnosť zobrazenia obrázku	file	Nie

6. Vnútroštátne predpisy – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
číslo predpisu podľa Zbierky zákonov	String (10)	Nie
vnútroštátny vykonávajúci predpis/požiadavka v sk (názov predpisu v sk)	Text	Áno

vnútroštátny vykonávajúci predpis/požiadavka v en (názov predpisu v en)	Text	Nie
dátum prvého uvedenia do platnosti	Date	Áno
dátum účinnosti poslednej novelizácie	Date	Áno
priamy odkaz na vnútroštátny právny predpis (url odkaz)	String (255)	Nie

7. *Harmonizované predpisy* – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
celexové číslo predpisu EÚ	String (15)	Áno
číslo predpisu EÚ	String (15)	Áno
druh EÚ predpisu (smernica/nariadenie)		
predpis EÚ v sk (názov predpisu)	Text	Áno
predpis EÚ v en (názov predpisu)	Text	Nie
odkaz na web EÚ pre danú výrobkovú skupinu	String (255)	Nie
vzťah/prepojenie na vnútroštátny vykonávajúci predpis/požiadavka (môže ich byť viac)	(vzťah)	Áno
vzťah/prepojenie na kategóriu vnútroštátneho predpisu	(vzťah)	Áno
rozsah vnútroštátneho právneho predpisu v sk	Text	Nie
rozsah vnútroštátneho právneho predpisu v en	Text	Nie
hlavné alebo špecifické požiadavky uvedené vo vnútroštátnom predpise v sk	Text	Nie
hlavné alebo špecifické požiadavky uvedené vo vnútroštátnom predpise v en	Text	Nie
orgán, v pôsobnosti ktorého je uvedený predpis, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)	Nie
spolugestor, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)	Nie
orgán trhového dohľadu, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)	Nie
vzťah/prepojenie na autorizované a notifikované osoby (môže ich byť viac)	(vzťah)	Nie

url harmonizovanej normy a príručky (môže ich byť viac)	String (255)	Nie
vzťah/prepojenie na číselník ukončenia posudzovania zhody (môže ich byť viac)	(vzťah)	Nie
url návodu (môže ich byť viac)	(vzťah)	Nie
vzťah/prepojenie na druh výrobku (môže ich byť viac)	(vzťah)	Áno
postupy posudzovania zhody (môže ich byť viac, atribút sa skladá z názvu a url)	String (255)	Nie
odkaz na url SNAS akreditácia (všeobecný odkaz)	String (255)	Nie
odkaz na modul M.3 Centrálny repozitár noriem (prepojenie na základe CELEX čísla EÚ predpisu alebo čísla EÚ predpisu)	(vzťah)	Nie
poznámka	Text (1500)	Nie
vzťah/prepojenie na číselník príklady výrobkov (môže ich byť viac)	(vzťah)	Nie
harmonizované oblasti podľa nariadenia (EÚ) 2019/1020	String (255)	Nie
vzťah/prepojenie na číselník postupy posudzovania zhody	(vzťah)	Nie

8. *Neharmonizovaná oblasť, špecifické* - atribúty vystupujúce v entite

Názov	Typ
vzťah/prepojenie na druh výrobku (môže ich byť viac)	(vzťah)
vzťah/prepojenie na vnútroštátny vykonávajúci predpis/požiadavka (môže ich byť viac)	(vzťah)
rozsah vnútroštátneho právneho predpisu v sk	Text
rozsah vnútroštátneho právneho predpisu v en	Text
hlavné alebo špecifické požiadavky uvedené vo vnútroštátnom predpise v sk	Text
hlavné alebo špecifické požiadavky uvedené vo vnútroštátnom predpise v en	Text
orgán, v pôsobnosti ktorého je uvedený predpis, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)
orgán trhového dohľadu, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)
vzťah/prepojenie na autorizované a notifikované osoby	(vzťah)

(môže ich byť viac)	
odkaz na url SNAS akreditácia (všeobecný odkaz)	String (255)
odkaz na url Centrálny repozitár noriem	String (255)
poznámka	Text (1500)
vzťah/prepojenie na číselník príklady výrobkov (môže ich byť viac)	(vzťah)

9. *Neharmonizovaná oblasť, všeobecné* – atribúty vystupujúce v entite

Názov	Typ
vzťah/ prepojenie na vnútroštátny vykonávajúci predpis/požiadavka (môže ich byť viac)	(vzťah)
rozsah vnútroštátneho právneho predpisu v sk	Text
rozsah vnútroštátneho právneho predpisu v en	Text
hlavné alebo špecifické požiadavky uvedené vo vnútroštátnom predpise v sk	Text
hlavné alebo špecifické požiadavky uvedené vo vnútroštátnom predpise v en	Text
podliehanie výrobku predchádzajúcemu povoleniu podľa vnútroštátneho práva	text (5000)
druh výrobku (môže ich byť viac)	(vzťah)
orgán, v ktorého pôsobnosti je uvedený predpis, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)
orgán trhového dohľadu, prepojenie na číselník organizácií (môže ich byť viac)	(vzťah)
vzťah/prepojenie na autorizované osoby (môže ich byť viac)	(vzťah)
odkaz na url SNAS	String (255)
odkaz na url Centrálny repozitár noriem	String (255)
poznámka	Text (1500)
vzťah/prepojenie na číselník príklady výrobkov (môže ich byť viac)	(vzťah)

10. *Príklady výrobkov* – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
-------	-----	--------------

názov výrobku v sk	String (255)	Áno
názov výrobku v en	String (255)	Nie

11. Druh osvedčenia o akreditácii – atribúty vystupujúce v entite

Názov	Typ	Povinné pole	Príklad
kód osvedčenia o akreditácii	String (4)	Áno	S
druh osvedčenia o akreditácii v sk	String (255)	Áno	skúšobné laboratórium
druh osvedčenia o akreditácii v en	String (255)	Áno	General requirements for the competence of testing and calibration laboratories (ISO/IEC 17025:2005)

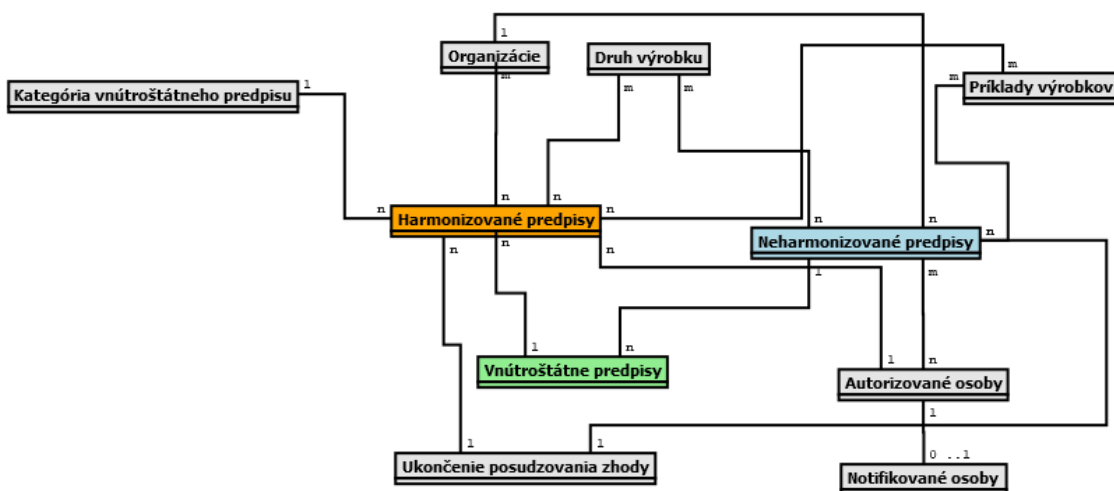
12. Skupina výrobkov (product family) – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
názov skupiny výrobkov	String (255)	Áno

13. Postupy posudzovania zhody (moduly) – atribúty vystupujúce v entite

Názov	Typ	Povinné pole
názov posudzovania zhody	String (255)	Áno

Príklad znázornenia vzťahov medzi číselníkmi:



Príklad niektorých číselníkov pre ilustráciu je v prílohe „prilohy/M2/ciselniky.zip“

Požiadavky na funkcionality manažmentu

1. V manažmente údajov sa bude dať zvoliť, aké atribúty sa budú zobrazovať vo vyhľadaných dátach vo verejnej časti aplikácie.
2. Používateľ bude môcť exportovať číselníky do xlsx, csv.
3. Používateľ bude môcť detail číselníka exportovať do pdf.
4. Používateľ bude môcť exportovať poprepájané dáta do xlsx.
5. Používateľ bude môcť nad existujúcimi číselníkmi vykonávať funkcie vytvorenia, úpravy, zneplatnenia a nahliadnutia.
6. Administrátor bude môcť vytvárať nové číselníky a prepájať ich s existujúcimi a novými číselníkmi.
7. Administrátor bude vytvárať prístupy jednotlivým členom organizácií, ktoré môžu editovať, vytvárať a zneplatňovať údaje vo svojej gescii.
8. Po úprave, vytvorení alebo zneplatnení údajov príde administrátorovi notifikácia na akceptovanie alebo neakceptovanie zmeny. Až po potvrdení administrátorom sa zmena prejaví na reálnych dátach.
9. Členovia organizácií sa budú prihlasovať do portálu 2FA.
10. Zamestnanci úradu sa budú prihlasovať do manažmentu aplikácie prostredníctvom LDAP a 2FA.
11. Manažment údajov sa bude zobrazovať na subdomena.unms.sk a bude nasadená vo vládnom Cloude Objednávateľa.
12. Administrátor bude môcť blokovať, vytvárať a upravovať členov organizácií.
13. O členoch organizácie, ktorých môže byť v jednej organizácii aj viac, budú uchované informácie ako meno, priezvisko, e-mail, organizácia, odbor/sekcia, telefónny kontakt.
14. Manažment údajov bude rozdelený do 3 sekcií. Každá sekcia bude mať svoj vlastný spôsob zobrazovania poprepájaných dát z databázy:
 - a) Pravidlá a požiadavky pre výrobky.
 - b) Technické predpisy z oblasti posudzovania zhody.
 - c) Spôsobilosť autorizovaných a notifikovaných osôb.

Nefunkčné požiadavky

1. Zhotoviteľ naplní databázu dátami, ktoré pripraví Objednávateľ.
2. Slovenská a anglická mutácia bude aj s hlavičkami a atribútmi tabuliek.

3. Interná časť aplikácie je v slovenskom jazyku. Do aplikácie sa budú vkladať dáta v slovenskom aj anglickom jazyku vrátane hlavičiek formulárov/tabuliek.

Požiadavky na funkcionality vyhľadávacej časti modulu

Vyhľadávanie bude umiestnené na webovom sídle Objednávateľa. Na webovom sídle Objednávateľa budú umiestnené tri typy vyhľadávania

1. Vyhľadávanie na stránke pre Pravidlá a požiadavky týkajúce sa výrobkov bude obsahovať viacero možností vyhľadávania:
 - a) Vyhľadávanie podľa druh výrobku z prednastaveného zoznamu výrobkov,
 - b) Vyhľadávanie vo vyhľadávacom poli, v ktorom zadá niektorý z nasledujúcich parametrov: číslo smernice, napr. 2014/53/EÚ, názov výrobku, časť názvu predpisu.
 - c) Vyhľadávať sa bude podľa atribútov - druh výrobku, názov vnútroštátneho predpisu, číslo vnútroštátneho predpisu, názov EÚ predpisu, číslo EÚ predpisu, ukončenie posudzovania zhody, názov organizácie.
 - d) Zadané výrazy môžu byť celé alebo neúplné slová/výrazy napr. hračk, 2014/53, hosp, označenie CE, vyhlásenie
 - e) Zoznam všeobecných predpisov
 - f) Ak používateľ nenájde, čo hľadá, systém ho odkáže na online formulár v module M4 Kontaktné miesto na výrobky.
 - g) Ilustračný príklad výsledkov vyhľadávania sa nachádza v prílohe „prilohy/M2/priklady_zobrazenia.docx.docx“.
 - h) Na každú vyhľadanú požiadavku sa bude dať kliknúť pre zobrazenie detailu informácií. V detaile sa budú zobrazovať dáta na základe nastavenia v manažmente, v ktorom administrátor vyberie, ktoré dáta sa majú zobrazovať. Ilustračný príklad výsledkov vyhľadávania sa nachádza v prílohe „prilohy/M2/priklady_zobrazenia.docx.docx“.
 - i) Vyhľadané veci sa budú môcť exportovať do pdf, xlsx na základe vyfiltrovaných dát alebo priamo na webe s možnosťou tlače.
 - j) Dáta budú prepojené prostredníctvom celexového čísla s Centrálnym repozitárom noriem (modul M3). Pri vyhľadaných dátach sa budú nachádzať normy, ktoré súvisia s daným harmonizovaným predpisom. Po kliknutí na normu sa používateľovi otvorí nové okno, kde sa prelinkuje na detail danej kliknutej normy.
 - k) Polia zobrazované vo výstupe z vyhľadávania:
 - len polia/atribúty, ktoré obsahujú (vyplnené) údaje
 - ak sa k jednému výrobku vzťahuje viacero predpisov a tieto predpisy majú vyplnené polia „rozsah pôsobnosti“ a „hlavné požiadavky“, tieto údaje sa zobrazia pre každý predpis samostatne.
2. Zobrazenie tabuľky Technické predpisy v oblasti posudzovania zhody
Na webovej stránke bude zobrazenie databázy v html formáte s možnosťou exportu do pdf formátu s atribútmi tak, ako v prílohe „prilohy/M2/technicke-predpisy-z-oblasti-posudzovania-zhody.pdf“ podľa zvolených parametrov.
3. Zobrazenie na stránke Spôsobilosť autorizovaných a notifikovaných osôb
Na webovej stránke bude zobrazenie databázy v html formáte s možnosťou exportu do pdf formátu s atribútmi tak, ako v prílohe „prilohy/M2/Sposobilost_AO_NO.pdf“ podľa zvolených parametrov.

Požiadavky na API pre data .gov.sk

API bude vytvorené z funkcií vyhľadávania v časti Pravidlá a požiadavky týkajúce sa výrobkov. Bude obsahovať základné číselníky a vzťahy, ktoré sú vytvorené medzi ostatnými číselníkmi. API bude mať

aj dokumentačnú časť, ktorá bude popisovať všetky dostupné RESTFull webové servery, napríklad prostredníctvom nástroja SWAGGER.

Požiadavky na autorizáciu prístupov

Požaduje sa, aby v aplikácii bolo možné hierarchické riadenie oprávnení a autorizácií jednotlivých užívateľov podľa pridelených rolí, a to minimálne v rozsahu:

1. Administrátor

- a) modifikuje, mení všetky údaje, pričom v logovaní sa tieto úpravy budú vždy evidovať ako zmeny vykonané administrátorom s menom,
- b) má prístup k všetkým aktuálnym, ako aj historickým údajom,
- c) modifikuje číselníky,
- d) riadi a nastavuje oprávnenia pre ostatných používateľov systému,
- e) spravuje integračnú platformu,
- f) má práva na hromadné úpravy údajov,
- g) má prístup k samotným údajom na úrovni databázového prístupu.

2. Kľúčový používateľ

- a) modifikuje, aktualizuje všetky evidované údaje, pričom v logovaní sa tieto úpravy budú vždy evidovať ako zmeny vykonané konkrétnym používateľom,
- b) má prístup k všetkým evidovaným aktuálnym, ako aj historickým údajom,
- c) tvorí a modifikuje šablóny reportov,
- d) má prístup k Informačnému systému,
- e) má právo modifikovať, meniť a opravovať,
- f) má prístup k všetkým aktuálnym údajom, ako aj historickým údajom,
- g) môže akceptovať aktualizované dáta do produkčných dát.

3. Člen organizácií

- a) modifikuje, aktualizuje všetky evidované údaje, ktoré patria pod jeho organizáciu,
- b) má prístup k všetkým svojim evidovaným aktuálnym, ako aj historickým údajom,
- c) môže si meniť heslo.

4. Používateľ

- a) číta a exportuje údaje.

Požiadavky na funkcionality

1. Podpora spracovania a zobrazovania údajov v slovenskej znakovej sade a podpora slovenského formátu času a metrických údajov.
2. Požaduje sa, aby užívateľské rozhranie bolo v slovenskom jazyku.
3. Prepojenie všetkých logovacích výstupov aplikácií, ktoré budú implementované v intranete Objednávateľa s existujúcim Log managerom Objednávateľa.
4. Aktivita používateľov musí byť zaznamenávaná formou auditného žurnálu tak, aby bolo možné kedykoľvek získať prehľad o tom, kto, kedy a aké aktivity v systéme vykonal.
5. Prezeranie auditných záznamov.
6. Vyhľadávanie v auditných záznamoch.
7. Automatické kopírovanie vybraných logov do externého úložiska (syslog).
8. Zhotoviteľ zabezpečí analytické a implementačné práce na vybraných častiach jednotnej digitálnej brány vrátane konfigurácie a vybudovania testovacieho prostredia daného riešenia.
9. Zhotoviteľ zabezpečí vypracovanie rámcovej špecifikácie Informačného systému (ktorá sa stane súčasťou Technického opisu riešenia).

10. Architektúra systému bude riešená v súlade so štandardom TOGAF. Architektonické pohľady budú dodané vo forme ArchiMate diagramov (alebo ekvivalent) rozdelené na nasledovné oblasti:
 - a) Biznis architektúra (používatelia, funkcie, procesy, služby).
 - b) Aplikačná architektúra (komponenty, procesy, aplikácie, funkcie, služby).
 - c) Architektúra údajov (údajové entity a ich vzťahy, tok údajov, príslušnosť údajov).
 - d) Technologická architektúra – časť systémová architektúra (uzly, komunikácia medzi uzlami, systémový softvér).
11. Prispôsobovanie vzhľadu rozmerom obrazovky – tzv. Responsible dizajn (PC, notebook, tablet, mobil).
12. Je nutné postupovať pri vytváraní design manuálu podľa jednotného dizajn manuálu dostupného na linku <https://idsk.gov.sk/>.

Všeobecné nefunkčné požiadavky

1. Otvorená architektúra pre efektívne zakomponovanie nových požiadaviek v súlade so zmenami legislatívy, doplnenie ďalších modulov s rozšírenou funkcionalitou, ktorá nie je predmetom tohto zadania.
2. Horizontálna a vertikálna škálovateľnosť.
3. Zabezpečenie vysokej dostupnosti pomocou cloudových riešení.
4. Jednotná integračná platforma.
5. Multiplatformové riešenie.
6. Softvérové riešenie technológií s otvoreným zdrojovým kódom.
7. Nezávislosť na platforme na strane klientskych počítačov.
8. Modulárne riešenie pre pokrytie procesu posudzovania vplyvov.
9. Štandardizácia vstupných údajov s cieľom zvýšenia integrity dát.
10. Možnosť dynamicky vytvárať zvolené štatistiky a reporty.
11. Dodržanie zásad a politiky informačnej bezpečnosti Objednávateľa.
12. Centrálneho monitoringu bezpečnosti riešenia a oprávnenosti prístupov.
13. Z pohľadu fyzickej architektúry riešenie predpokladá pre aplikácie implementované do extranetu využitie infraštruktúrnych a hardvérových kapacít vládneho cloudu.
14. Zhotoviteľ zabezpečí na svojom HW vývoj a testovanie prevádzky systému.
15. Objednávateľ zabezpečí testovacie prostredie výpočtových prostriedkov cez <http://www.sk.cloud/>, kde je možné získať viac informácií o fyzickom a logickom usporiadaní prostredia.
16. Návrh a realizácia riešenia, ktoré bude plne kompatibilné s daným a dostupným prostredím. Návrh na úrovni HW sa očakáva vo forme návrhu nutných výpočtových kapacít a parametrov, ako aj prepojenia jednotlivých virtuálnych prostriedkov.
17. Zhotoviteľ musí zabezpečiť dodávku tak, aby sa minimalizovalo riziko tzv. Vendor-locku.
18. Od riešenia sa očakáva, že sa výkonnostne nadimenzuje tak, aby dokázalo v zmysle štandardov informačných systémov verejnej správy plnohodnotne obslúžiť používateľov podľa nasledovného rozdelenia: Používatelia intranetu - min. 50 osôb, používatelia verejného portálu - všetci občania, ktorí využívajú funkcionalitu daného riešenia, ich počet nie je možné inak obmedziť.

Požiadavky na dizajn

1. Dizajn verejnej časti modulov bude podliehať princípom pre návrh a rozvoj elektronických služieb verejnej správy (dostupné na <https://idsk.gov.sk/>).
2. Návrh a vyhotovený dizajn bude Zhotoviteľ predkladať na pripomienkovanie Objednávateľovi.

Identifikácia a autentifikácia používateľa

1. Identifikácia a autentifikácia používateľa pomocou mena a hesla a následné pridelenie rolí.
2. Prístup používateľov musí byť riadený na základe funkčných a dátových oprávnení. Modul musí byť integrovaný s centrálnym systémom riadenia identít Objednávateľa LDAP, v rámci ktorého sú evidovaní všetci zamestnanci a ich zaradenie do príslušných rolí a pracovných pozícií.
3. Správa užívateľov bude riešená samostatne pre každú oblasť/modul.

Požiadavky na implementáciu

Spracované údaje musia byť uložené v relačnej databáze umožňujúcej viacnásobný súčasný prístup a transakčné spracovanie (napr. MariaDB alebo PostgreSQL). Implementácia modulu musí byť realizovaná v niektorom z jazykov - ideálne PHP alebo aj Python, Java openjdk. Webové rozhranie môže využívať Javascript, musí byť v súlade so špecifikáciami HTML5 a CSS a plne funkčné minimálne v aktuálnych verziách prehliadačov Mozilla Firefox, Google Chrome a Microsoft Edge.

Požiadavky na testovanie

Požaduje sa, aby testovacie princípy použité pri testovaní aplikácií, modulu a Informačného systému vychádzali so štandardov ISTQB alebo ekvivalentného štandardu. Ďalej sa požaduje vypracovanie stratégie testovania a plánu testov IS, ktoré určia najmä:

1. Detailný časový rámec testovania
2. Popis testovania a testovacích scenárov
3. Zodpovednosti počas testovania
4. Testovacie fázy
5. Kritériá na akceptačné testovanie v súlade so Zmluvou o dielo.

Požaduje sa testovanie systému ako celku, ale aj jeho jednotlivých častí podľa schváleného plánu testov testovacími dátami vyhodnotenými Zhotoviteľom:

Typ testu	Zodpovednosť	Požiadavky na dodávateľa
Funkčné testy	Zhotoviteľ	Príprava, realizácia a vyhodnotenie testov
Bezpečnostné testy	Zhotoviteľ	Príprava, realizácia a vyhodnotenie testov
Integračné testy	Zhotoviteľ	Príprava, realizácia a vyhodnotenie testov
Usability Testy	Zhotoviteľ	Príprava, realizácia a vyhodnotenie testov
Akceptačné testy	Objednávateľ	Súčinnosť a podpora pri príprave, realizácii a vyhodnotení testov
Penetračné testy	Zhotoviteľ	Príprava, realizácia a vyhodnotenie testov
Finálne akceptačné testovanie	Objednávateľ	Súčinnosť a podpora pri príprave, realizácii a vyhodnotení testov

Zhotoviteľ pred začiatkom procesu testovania v rámci analýzy vytvorí plán testovania pre Informačný systém.

Plány testov obsahujú popis prístupu k testovaniu všetkých komponentov a položiek vyplývajúcich z opisu predmetu zákazky. Tieto dokumenty pokrývajú manažérske plánovanie (organizácia, časový priebeh), ako aj technické plánovanie (typ testov, druhy testov, testovacie prostredie, testovacie dáta, **testovacie scenáre, testovacie prípady**).

Funkčné testy - overenie správnosti a úplnosti jednotlivých funkcií implementovaných častí systému, teda či reálne správanie sa systému presne zodpovedá tomu, ako je popísané vo funkčnej špecifikácii riešenia vrátane testovania dátovej kvality a úplnosti z nasadenia BETA verzie modulov do testovacieho prostredia na strane Zhotoviteľa, príprava testovacích scenárov a testovacích dát, ako aj vlastný výkon testov a ich vyhodnotenie a zaznamenanie.

Bezpečnostné testy: naplnenie cieľa - preverenie systému v prípade možných zásahov do bezpečnosti prevádzky a dát aplikácie.

Záťažové a výkonnostné testovanie: vykonávané pomocou nástrojov a automatizovaných skriptov nad produkčným a testovacím prostredím pre vybrané reprezentatívne kritické funkcionality systému. Testy majú emulovať rôzne typy používateľských a automatizovaných vstupov na hostiteľskom systéme, ktorého výkon má byť testovaný. Zachytené výsledky výkonnostných a záťažových testov budú vzájomne porovnávané. Testovanie má prebiehať v jednotlivých sekvenciách, pri ktorých sa bude postupne zvyšovať zaťaženie systému (stress test). Tento nárast bude realizovaný so sledovaním chybovosti vrátených odoziev testovaného systému. Pri realizácii výkonnostného a záťažového testovania bude posudzovaná výkonnosť a kapacita riešenia. Pri výkonnostnom a záťažovom testovaní majú byť výsledky posudzované aj vzhľadom na plánovaný počet interných používateľov systému a počet odhadovaných konkurenčných prístupov.

Systémové a integračné testovanie: overenie naplnenia požiadaviek na integráciu s externými systémami. Testovacie scenáre musia pokrývať všetky identifikované a implementované externé rozhrania systému. Je potrebné realizovať pozitívne aj negatívne (sunny-day, rainy-day) integračné scenáre.

Používateľské testy funkčného používateľského rozhrania (UX testovanie) - testy použiteľnosti (usability) koncových služieb: Testovanie kompatibility prehliadačov - overenie miery kompatibility s bežne používanými internetovými prehliadačmi v ich základnej konfigurácii. Požaduje sa pre verejnú (extranet) a aj pre privátnu (intranet) časť portálu na bežných webových prehliadačoch – MS Edge, Mozilla Firefox, Google Chrome, Opera, Apple Safari (všetky verzie vymenovaných prehliadačov, ktoré nie sú staršie ako 4 roky).

Finálne akceptačné testovanie – vykonanie testovacích scenárov na finálnej verzii systému realizované po vyladení systému a odstránení zistených chýb z predošlých testov. Účelom finálnych akceptačných testov je overenie zo strany objednávateľa, že navrhnuté a implementované riešenie je pripravené na nasadenie do prevádzky. Testovanie môže prebiehať na Objednávateľom odsúhlasenej podmnožine testovacích scenárov, pričom akceptačné kritériá majú byť vopred definované. Výsledky testovania môžu určiť dodatočné nezrovnalosti medzi implementovaným riešením a jeho špecifikáciou, ako aj potrebu korekcie zo strany Zhotoviteľa pred nasadením do prevádzky alebo počas prevádzky (na základe závažnosti zistení a dohody s Objednávateľom).

Dokumentácia testovania, ktorá prebieha počas celej fázy testovania, udržiava Plán testov, testovacie scenáre a prípady, vedie zoznam neuzavretých defektov.

Požiadavky na projektové riadenie a projektové výstupy

Požaduje sa, aby projektové riadenie na strane Zhotoviteľa bolo realizované a všetky projektové výstupy boli dodávané v súlade s vyhláškou Úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky MIRRI SR č. 546/2021 Z. z. a Aktualizovanou metodikou projektového riadenia projektov informatizácie verejnej správy.

Minimálne projektové výstupy sú nasledovné:

P0 - Rámcový návrh riešenia

1. Analýza súčasného stavu
 - a) Legislatíva
 - b) Procesy a služby – procesná analýza
 - c) Existujúce informačné systémy, aplikácie, rozhrania
 - d) Existujúce dáta a ich migrácia v rámci projektu
 - e) Existujúca IKT Infraštruktúra
2. Popis koncepcie navrhovaného riešenia
3. Logická schéma navrhovaného riešenia
4. Popis komponentov zobrazených v logickej schéme
5. Odhadovaná náročnosť jednotlivých modulov v MD
6. Podrobný štruktúrovaný položkový rozpočet
7. Popis a špecifikáciu navrhovaných parametrov pre SLA.

P1 - Detailný návrh riešenia (DNR)

Minimálny rozsah: 10 strán bez príloh

Zoznam kapitol:

1. Architektúra riešenia projektu
 - a) Biznis vrstva
 - b) Aplikačná vrstva
 - c) Dátová vrstva, dátový rozsah projektu, opis dátovej architektúry riešenia, dátový model
 - d) Funkčné komponenty
 - e) Referenčné, otvorené, analytické, moje údaje
 - f) Technologická vrstva
 - g) Integračná vrstva
2. Mapovanie a analýza funkčných požiadaviek – detailný návrh riešenia
 - a) Katalóg funkčných požiadaviek
3. Mapovanie a analýza technických požiadaviek – detailný návrh riešenia
 - a) Katalóg technických požiadaviek (inf. bezpečnosť, rozhrania a pod.)
 - b) Požiadavky na migráciu dát
4. Požiadavky na vizuálne komponenty (GUI)
 - a) Vytvorenie informačnej architektúry a mapovanie používateľskej cesty
 - b) Vytvorenie prototypu používateľského rozhrania viacerými iteráciami
5. Požiadavky na nevizuálne komponenty (OpenAPI)
6. Bezpečnostná architektúra
7. Závislosti na ostatných IS/Projektoch
8. Zdrojové kódy

P2 - Plán testov

Minimálny rozsah: 5 strán bez príloh

Zoznam kapitol:

1. Opis produktu a jeho komponentov
2. Štruktúrovaný opis úrovni testovania celého riešenia a jeho komponentov
3. Organizácia testov a personálne zabezpečenie
4. Typy a druhy testov celého riešenia a jeho komponentov
 - a) Testovacie prípady/scenáre a ich namapovanie na katalóg požiadaviek
 - b) Testovacie prostredie
 - c) Testovacie dáta
 - d) Testovacie záznamy a protokoly
5. Klasifikácia chýb
6. Manažment riadenia chýb a opráv
7. Monitoring a reporting testovania
8. Spôsoby vyhodnotenia výsledkov testovania

P3 - Testovanie

Minimálny rozsah: 10 strán

Zoznam kapitol:

1. Funkčné testovanie (FAT)
2. Systémové a integračné testovanie
3. Závažové a výkonnostné testovanie
4. Bezpečnostné testy
5. Používateľské testy funkčného používateľského rozhrania (UX testovanie)
6. Používateľské akceptačné testovanie (UAT)
7. Testovacie scenáre overenia migrovaných údajov
8. Finálne akceptačné testovanie

P4 - Školenia personálu

Minimálny rozsah: 5 strán

Zoznam kapitol:

1. Školiace prostredie
2. Školiace materiály pre administrátorov a používateľov

P5 – Dokumentácia k IS

Minimálny rozsah: 5 strán bez príloh

Zoznam kapitol:

1. Aplikačná príručka
2. Používateľská príručka
3. Inštalčná príručka a pokyny na inštaláciu (úvodnú/opakovanú)
4. Konfiguračná príručka a pokyny pre diagnostiku
5. Integračná príručka
6. Prevádzkový opis a pokyny pre servis a údržbu
7. Pokyny na obnovu pri výpadku alebo havárii (Havarijný plán)
8. Bezpečnostný projekt na modul

Požiadavky na realizáciu školení

Požaduje sa vytvorenie a dodanie elektronických školiacich materiálov pre technický personál, administrátorov a používateľov. Zo zrealizovaných školení je nevyhnutné predložiť prezenčné listiny. Školiacu miestnosť pre realizáciu školení zabezpečí Objednávateľ, pričom všetky ostatné náklady na prípravu a realizáciu školenia a školiacich materiálov znáša Zhotoviteľ.

Názov školenia	Trvanie školenia v dňoch
Školenie pre technický personál	2
Školenie pre administrátorov a používateľov	3

Obsahom musia byť prebrané procesy realizované danou skupinou používateľov a ponechaný dostatočný čas na diskusiu a individuálne otázky ohľadne špecifik systému. Vytvorenie a sprístupnenie školiacich materiálov bude vo forme, ktorá umožní ich priebežné dopĺňanie a aktualizáciu.

Požiadavky na bezpečnosť

Návrh a implementácia musí využívať techniky, ktoré eliminujú alebo minimalizujú pravdepodobnosť, že výsledné dielo bude obsahovať bežné zraniteľnosti webových aplikácií (ako napr. SQL injection, cross-site scripting, session hijacking, a pod.). Vyžaduje sa súlad s bezpečnostnými požiadavkami OWASP ASVS. Požaduje sa, aby boli všetky časti Diela realizované v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a aby bol zabezpečený jeho súlad s požiadavkami zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. Komunikácia bude zabezpečená prostredníctvom protokolu https, zabezpečeného certifikátu podpísaného certifikačnou autoritou. Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty. Webová stránka musí obsahovať bezpečnostné prvky, najmä ochranu webového prostredia, databáz a prístupu (napr. uložené dokumenty sa nenachádzajú v root aplikácii, aplikácie by mali používať CSRF tokeny o veľkosti 128 bitov a iné). Požaduje sa, aby aplikácie boli prevádzkované v súlade s bezpečnostným projektom Zhotoviteľa, s bezpečnostnými požiadavkami podľa aktuálne platnej legislatívy, v súlade so štandardami platnými pre informačné systémy verejnej správy, ako aj uznávanými bezpečnostnými normami.

V rámci bezpečnostnej politiky Objednávateľa sú kladené požiadavky na bezpečnosť a spôsob uchovávaní údajov v Informačnom systéme. Pri kľúčových moduloch je preto vyžadované uchovávanie záznamu o činnosti používateľov, čo zabezpečuje tiež možnosti vyvodenia dôsledkov v prípade prieniku do systému a pomáha identifikovať bezpečnostné riziká. Vzhľadom na to, že systém bude prijímať a spracovávať dokumenty a súbory, vyžaduje sa ochrana systému pred škodlivým kódom minimálne v rozsahu § 33 vyhláškou Úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky MIRRI SR č. 546/2021 Z. z. Taktiež je požadované rozdelenie infraštruktúry do zón na sieťovej úrovni, čo pri prieniku do verejnej časti systému zabraňuje úniku privátnych dát. V rámci IT platformy sa tiež požaduje vyriešiť zálohovanie kritickej infraštruktúry a ochranu pred preťažením alebo stratou údajov.

Požiadavky na nasadenie do prevádzky

Súčasťou dodávky riešenia je zabezpečenie kompletnej inštalácie riešenia do produkčného prostredia zákazníka. Táto spočíva v inštalácii operačných systémov, databáz, podporného softvéru, aplikácií, ich

konfigurácie a vzájomného prepojenia tak, aby bolo umožnené bezproblémové prevádzkovanie kompletnej funkcionality dodávaného riešenia vo vládnom Cloude aj na intranete Objednávateľa.

Technologická architektúra

Riešenie IS jednotnej digitálnej brány pre Objednávateľa určenej pre verejnosť bude postavené a nasadené vo vládnom Cloude. Systém bude prevádzkovaný Objednávateľom a k dispozícii bude dostatočný výkon pre zabezpečenie spoľahlivej prevádzky. Súčasťou projektu bude využitie nasledovnej infraštruktúry vo vládnom Cloude:

1. redundantné riešenie aplikačných a databázových serverov,
2. zabezpečenie LAN infraštruktúry,
3. zabezpečenie SAN infraštruktúry,
4. zabezpečenie GovNet konektivity
5. virtualizácia prostredia,
6. zabezpečenie zálohovania.

Pri budovaní aplikačných komponentov v rámci navrhovaného riešenia sa predpokladá využitie služieb vládneho Cloudu. Malo by ísť minimálne o model využívania IaaS, pri ktorom cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry - ako serverov, úložísk údajov a sieťovej infraštruktúry.

Pre úspešné nasadenie a prevádzku systému sa využijú nasledujúce eGovernmentové cloudové služby PaaS:

1. Služby konfiguračného manažmentu,
2. Služby pre riadenie procesu nasadzovania nových verzií a ich aktualizácie,
3. Služby vývojového aplikačného manažmentu a testovacieho prostredia,
4. Správa testovacích scenárov a plánovanie testov,
5. Služby správy a konfigurácie softvéru,
6. Služby pre dohľad nad plynulou a bezpečnou prevádzkou systému.

V rámci Cloudového riešenia bude Zhotoviteľom zabezpečené:

1. Dokonfigurovanie svojej časti do Virtual Log server - Server na zber systémových/aplikačných logov pre dosiahnutie vysoko kvalitnej správy a debugovania v prípade nežiaducich problémov a zabezpečenie vyššej úrovne kybernetickej bezpečnosti. Softvérový produkt závisí od výberu technológie uchádzača o modul M3.
2. Dokonfigurovanie svojej časti do Virtual monitoring server – Monitorovací server pre zabezpečenie kvality bežiacich služieb, ktorý bude schopný po napojení na všetky virtuálne servery zasilať prípadné notifikácie o ich stave pomocou e-mailovej komunikácie priamo administrátorovi systému. Zabezpečí sa tak vysoká úroveň informovanosti o stave systému a včasné odhalenie problémov najmä v podobe výpadkov služieb a systému. Odporúčaný server je Zabbix, prípadne je možné použiť Nagios alebo iné. Softvérový produkt závisí od výberu technológie uchádzača o modul M3.
3. Dokonfigurovanie svojej časti do Virtual security audit server – VAS server, pomocou ktorého bude možné zvýšiť kybernetickú bezpečnosť systému a zabezpečiť centralizovanú správu inštalovaných aktualizácií a bezpečnostných záplat. V rámci funkcií bude v pravidelných intervaloch vyhodnocovať stav operačných systémov a bežiacich aplikácií virtuálnych serverov a informovať aj pomocou e-mailovej komunikácie administrátora systému. Odporúčaným VAS

serverom je OpenVAS, poprípade iné. Softvérový produkt závisí od výberu technológie uchádzača o modul M3.

4. Dokonfigurovanie svojej časti do Virtual Firewall router – V prípade nedostatočne zabezpečenej siete žiadateľa a vzhľadom na povahu a charakter projektu, kde sa neuvažuje o zabezpečení celej siete žiadateľa, je v prípade pochybností o kvalite bezpečnosti siete možné využiť virtuálny softvérový firewall router pre kvalitné zabezpečenie kybernetickej bezpečnosti na sieťovej úrovni. Odporúčaným systémom je PfSense ktorý ponúka množstvo potrebných funkcií, ako aj dvojfaktorovú autentifikáciu VPN prístupu. Softvérový produkt závisí od výberu technológie uchádzača o modul M3.

Vo virtuálnom prostredí sa uvažuje o ako hlavnom prístupovom bode s virtuálnym firewall router serverom – smerovači s funkciami firewall-u, ktorý bude centrálnym bodom, cez ktorý bude prebiehať komunikácia smerom in a out cez WLAN port, zároveň bude zabezpečovať VPN koncentrátor, DNS a bezpečný a riadený inter vlan routing medzi dvoma internými privátnymi sieťami vlan Management a vlan private, ku ktorým sú priradené rovnomenné virtuálne switche – prepínače. Podsieť pre management zabezpečuje bezpečnú komunikáciu riadiaceho toku dát medzi jednotlivými virtuálnymi servermi a zároveň sieť pre zálohovanie, kontrolu a synchronizáciu. Podsieť private zabezpečuje konektivitu pre aplikačný tok dát, ktorý je z bezpečnostných dôvodov oddelený od ostatných v rámci management podsiete.

Požiadavky na zálohovanie a riešenie obnovy

1. Zálohovanie produkčného prostredia, ako aj jeho prípadnú obnovu zabezpečuje Zhotoviteľ následne po každej implementovanej a akceptovanej zmene v systéme formou zálohy celej entity virtualizovaného prostredia, v ktorom nastala zmena na médiu.
2. Zálohovanie dát uložených v databáze bude riešené automaticky nastavením zálohovacích pravidiel Objednávateľa.
3. Administrátorom Objednávateľa bude sprístupnená konzola nad databázovým prostredím, v ktorej budú administrované samotné pravidlá na zálohovanie, prípadne na obnovu údajov.
4. Zálohovanie postačuje riešiť tak, aby bolo možné obnoviť prevádzku v priebehu jedného pracovného dňa odo dňa vzniku takejto potreby.
5. Požaduje sa vykonávať týždenné zálohovanie, a to v rozsahu úplnej zálohy virtualizovaného prostredia.
6. Požaduje sa zabezpečiť dostupnosť poslednej úplnej zálohy. Komplexné zálohovanie dát sa požaduje vykonávať raz mesačne. Priebežné zálohovanie údajov bude vykonané každodenne, a to v nočných hodinách.
7. Zálohovanie modelov a reportov - každý deň.
8. Doba obnovy zo zálohy do 8 hodín.
9. Využiť možnosti a služby vládneho Cloudu pri zálohovaní.

Požiadavky na SW licencie a licenčné požiadavky

Zhotoviteľ v rámci dodania Diela dodá všetky potrebné licencie, ktoré Objednávateľ potrebuje k používaniu Diela pre neobmedzený počet užívateľov.

Udelenie výhradnej licencie Objednávateľovi ako nadobúdateľovi na použitie diela, teda Predmetu Zmluvy, t. j. licencie bez vecného alebo územného obmedzenia na neobmedzený čas na každý spôsob použitia diela.

1. Ak Zhotoviteľ v rámci plnenia predmetu Zmluvy vytvorí a implementuje Objednávateľovi Dielo, vo vzťahu ku ktorému Zhotoviteľ je alebo bude oprávneným držiteľom akýchkoľvek práv duševného vlastníctva podľa príslušných aplikovateľných právnych predpisov (ďalej len „Autorské dielo“), Zhotoviteľ Objednávateľovi udelí právo na užívanie Autorského diela, a to

v rozsahu potrebnom pre realizáciu a riadne užívanie Autorského diela (ďalej len „licencia“). Zhotoviteľ dodá Objednávateľovi licenciu ako výhradnú, v neobmedzenom kvantitatívnom, vecnom a územnom rozsahu, a to všetkými do úvahy prichádzajúcimi spôsobmi a s časovým rozsahom obmedzeným iba dobou trvania majetkových práv k takémuto Autorskému dielu.

2. V prípade, že v rámci plnenia predmetu Zmluvy Zhotoviteľ dodá a/alebo implementuje Autorské dielo, vo vzťahu ku ktorému Zhotoviteľ nie je držiteľom alebo poskytovateľom práv na jeho používanie, je Zhotoviteľ povinný zabezpečiť práva na jeho používanie (u príslušného držiteľa alebo poskytovateľa týchto práv) pre Objednávateľa v nutnom rozsahu pre funkčné použitie systému. Splnenie tejto povinnosti je Zhotoviteľ povinný Objednávateľovi riadne preukázať pred odovzdaním príslušnej služby a/alebo Autorského diela.
3. Požaduje sa, aby Zhotoviteľ v prípade plnenia predmetu budúcej zmluvy prehlásil, že má práva na Autorské dielo a plnením predmetu budúcej zmluvy neporušuje žiadne práva duševného vlastníctva iných osôb a je oprávnený s prípadnými právami duševného vlastníctva nakladať, inak zodpovedá za škodu tým spôsobenú. Budúci Zhotoviteľ sa súčasne musí zaviazat' na vlastné náklady vykonať všetky účinné opatrenia na ochranu svojich práv duševného vlastníctva, ako aj ochranu práv vyplývajúcich Objednávateľovi z poskytnutej licencie.

Forma a spôsob odovzdania predmetu zmluvy

Zhotoviteľ dodá technologické riešenie vrátane konfigurácie, inštalácie SW vo vládnom Cloude, ktoré je nevyhnutné pre implementáciu projektu a jeho zavedenie do rutinej prevádzky podľa detailnej funkčnej, technickej špecifikácie a projektového plánu.

Odovzdanie a prevzatie Informačného systému sa bude uskutočňovať postupne, a to v termínoch podľa časového harmonogramu dodávky Diela.

K Informačnému systému bude dodaný technický návrh - high a low level design nasadenia do infraštruktúry Objednávateľa (nasadenie do Cloudu).

Zhotoviteľ vypracuje a dodá produktovú dokumentáciu:

1. **Technickú dokumentáciu** v slovenskom jazyku a v elektronickej forme na CD/DVD, ktorá bude obsahovať:
 - a) popis integračnej, aplikačnej a technickej architektúry,
 - b) väzby na iné systémy,
 - c) popis tokov dát,
 - d) procesné modely elektronických služieb
2. **Prevádzkovú dokumentáciu** v slovenskom jazyku a v elektronickej forme na CD/DVD, ktorá bude obsahovať:
 - a) chybové stavy a postup ich riešenia,
 - b) postup mechanizmu riadenia prístupu užívateľov k dátam a funkciám aplikácie,
 - c) popis procedúr pre zálohu a obnovu dát.
3. **Používateľskú dokumentáciu** v slovenskom jazyku v elektronickej forme na CD/DVD, ktorá bude obsahovať:
 - a) popis počítačového programu a jeho funkcií,
 - b) postupy a úkony potrebné pre riadenie a používanie aplikácie,
 - c) chybové a neštandardné stavy a dostupné spôsoby ich riešenia.

Špecifikácia záručného servisu

Záruka v trvaní 24 mesiacov odo dňa podpisu Záverečného akceptačného protokolu. V prípade zistenia väd Diela počas trvania zmluvnej záruky je Zhotoviteľ povinný odstrániť zistené vady

na vlastné náklady bezodkladne po ich oznámení. Zhotoviteľ sa zaväzuje začať s odstraňovaním riadne nahlásených väd podľa podmienok uvedených v Zmluve. Za nástup na odstránenie vady sa rozumie pripojenie sa Zhotoviteľa cez vzdialený prístup alebo príchod k Objednávateľovi na miesto výskytu vady (on-site). Zhotoviteľ zabezpečuje službu HelpDesk pre správcov systému, ktorá slúži k hláseniu väd, ako aj dokumentovaniu ich priebehu a riešenia. Objednávateľ má prístup k tejto službe a prostredníctvom nej eviduje svoje hlásenia. Zhotoviteľ je povinný pre Objednávateľa zabezpečiť a umožniť mu zadanie reklamácie riešenia požiadavky prostredníctvom služby HelpDesk.

Ochrana osobných údajov

Ak Informačný systém bude spracovávať osobné údaje, musí spĺňať legislatívne požiadavky dané nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, ako aj zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a vyhlášky Úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky MIRRI SR č. 546/2021 Z. z.

Na splnenie týchto požiadaviek Zhotoviteľ vypracuje bezpečnostnú dokumentáciu (bezpečnostný projekt), ktorá musí obsahovať najmä:

1. Analýzu spracúvania osobných údajov, ktorej úlohou bude analyzovať výskyt a spôsob spracúvania osobných údajov využívaných v rámci riešenia, posúdiť riziká pre práva a slobody fyzických osôb.
2. Návrh bezpečnostných opatrení – tzn. primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania osobných údajov, pričom sa požaduje, aby sa prihliadalo najmä na použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť Informačného systému podľa § 39 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Požiadavky na súlad s legislatívou a súvisiacimi dokumentami

Požaduje sa, aby Informačný systém a všetky projektové výstupy boli v súlade s platnou a účinnou legislatívou a súvisiacimi dokumentami:

1. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
2. Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
3. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
4. Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
5. Vyhláška Úradu podpredsedu vlády SR pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky MIRRI SR č. 546/201 Z. z.

6. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 85/2020 Z. z. o riadení projektov v znení vyhlášky MIRRI SR č. 545/2021 Z. z.
7. STN ISO/IEC 2701- Informačné technológie, Bezpečnostné metódy, Systémy riadenia informačnej bezpečnosti, Požiadavky, (STN ISO/IEC 27001:2014).
8. Národná koncepcia informatizácie verejnej správy - <https://rokovania.gov.sk/RVL/Resolution/19750/1>.
9. Aktualizovaná metodika projektového riadenia projektov informatizácie verejnej správy (dostupná na <https://www.mirri.gov.sk/projekty/projekty-esif/operacny-program-integrovana-infrastruktura/prioritna-os-7-informacna-spolocnost/metodicke-dokumenty/metodika-riadenia-qa-projektov-informatizacie-verejnej-spravy/index.html>).
10. Metodika riadenia QA projektov informatizácie verejnej správy (dostupná na <http://www.informatizacia.sk/metodika-riadenia-qa-projektov-informatizacie-verejnej-spravy/26689c>).
11. Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (dostupná na https://www.csirt.gov.sk/wp-content/uploads/2021/08/MethodikaZabezpeceniaIKT_v2.1.pdf).
12. Katalóg služieb a požiadavky na realizáciu služieb vládneho cloudu (dostupné na [Katalóg cloudových služieb | Vicepremier \(gov.sk\)](#)).
13. Používateľské princípy pre návrh a rozvoj elektronických služieb verejnej správy (dostupné na <https://idsk.gov.sk/> a https://www.mirri.gov.sk/wp-content/uploads/2019/04/Methodick%C3%A9-usmernenie-pre-tvorbu-pou%C5%BE%C3%ADvate%C4%BEsky-kvalitn%C3%BDch-elektronick%C3%BDch-slu%C5%BEieb-verejnej-spr%C3%A1vy_v2.pdf).