

Tehnična specifikacija – Prenova informacijske rešitve IBIS++/OT portal ter njeno vzdrževanje

Borzen, d.o.o.

Seznam kratic

Kratica	Opis
2FA	Dvofaktorska avtentikacija
OT	Operater trga.
CMS	Sistem za upravljanje vsebin.
DNN	Dotnetnuke sistem za upravljanje vsebine in spletnih aplikacij.
MVVM	Strukturni oblikovalski vzorec.
TLS	Kriptografski protokol za varno komunikacijo v omrežju (npr. HTTPS/TLS).
CRUD	Štiri osnovne operacije nad podatki: ustvarjanje (Create), branje (Read), posodabljanje (Update) in brisanje (Delete).
API	Aplikacijski programski vmesnik.
SQL	Strukturirani povpraševalni jezik za delo s podatkovnimi bazami.
JS	Objektni skriptni programski jezik.
XML	Razširljivi označevalni jezik, ki omogoča format za opisovanje strukturiranih podatkov.
GDPR	Splošna uredba o varstvu podatkov (Uredba (EU) 2016/679).
Cneg	Negativna osnovna cena.
Cpoz	Pozitivna osnovna cena.
SIPX	Slovenski borzni indeks.
MWh	Fizikalna enota megavatna ura.
DO	Distribucijski operater.
EIC	Identifikacijska oznaka člana bilančne sheme.
BS	Bilančna skupina.
BPS	Bilančna podskupina.
OBS	Odgovorni bilančne skupine.
OBPS	Odgovorni bilančne podskupine skupine.
HTML	(Hypertext Markup Language) je označevalni jezik za izdelavo spletnih strani.
SO	Sistemi operater.
IIS	(Internet Information Services) razširljiva programska oprema spletnega strežnika.
GUID	(Universally unique identifier) je globalno enolični identifikator.
URL	(Uniform Resource Locators) je spletni naslov.
VR	Vozni red.
MDM	(master data management) baza partnerjev in kontaktov.
PPM	Prezemno predajno mesto.
POZ	Pozitivno.
NEG	Negativno.
TP	Tržni plan.
SAOP	Sistem iCenter SAOP.
ERP	(Enterprise resource planning) načrtovanje virov v podjetju.
EIS	Enotni informacijski sistem.
SMTP	(Simple Mail Transfer Protocol) je protokol za prenos elektronske pošte.
LPBO	Letni poračun bilančnega obračuna.
BO	Bilančni obračun.
SSO	Enotna prijava (Single Sign-On).

MFA	Večfaktorska avtentikacija (Multi-Factor Authentication).
OIDC	OpenID Connect.
OAuth 2.0	Protokol za avtorizacijo (OAuth 2.0).
OpenAPI	Specifikacija za opis API vmesnikov (OpenAPI).
RPO	Cilj obnovitvene točke (Recovery Point Objective).
RTO	Cilj obnovitvenega časa (Recovery Time Objective).
DR	Obnova po nesreči (Disaster Recovery).
BCP	Načrt neprekinjenega poslovanja (Business Continuity Plan).
SIEM	Sistem za upravljanje varnostnih informacij in dogodkov (Security Information and Event Management).
SOC	Varnostno-operativni center (Security Operations Center).
SAST	Statično testiranje varnosti aplikacije (Static Application Security Testing).
DAST	Dinamično testiranje varnosti aplikacije (Dynamic Application Security Testing).
SBOM	Seznam programskih komponent (Software Bill of Materials).
HSM	Strojni varnostni modul (Hardware Security Module).
PAdES	Standard za podpisovanje PDF dokumentov (PDF Advanced Electronic Signatures).
XAdES	Standard za podpisovanje XML dokumentov (XML Advanced Electronic Signatures).
LLM	Veliki jezikovni model (Large Language Model).

1. Uvod

1.1. Kontekst in namen projekta

Naročnik (Borzen, d.o.o.) kot operater trga z elektriko deluje v okolju strogih regulatornih zahtev in kritične infrastrukture, sam Borzen pa je opredeljen kot izvajalec bistvenih storitev. Poslovno okolje ter energetska zakonodaja (ZOEE, Energetski zakon EZ-2, Zakon o uvajanju naprav za proizvodnjo električne energije iz obnovljivih virov viri - ZUNPEOVE ter drugi podzakonski akti) narekujejo visoko stopnjo digitalizacije in zanesljivosti procesov. Borzenove ključne naloge v vlogi operaterja trga so upravljanje bilančne sheme, evidentiranje zaprtih pogodb in obratovalnih napovedi, organiziranje platforme operaterja trga za izravnalno energijo, zbiranje, analizo in objavo podatkov z namenom zagotavljanja preglednosti delovanja trga z električno energijo ter, kar je najpomembnejše z vidika tega naročila, izvajanje bilančnega obračuna in poravnave poslov, povezanih z omenjenimi nalogami.

Za izvajanje nalog povezanih s postopkom bilančnega obračuna ter določenih ostalih zadolžitev iz nabora nalog operaterja trga se uporablja informacijsko rešitev poimenovano IBIS++. Gre za informacijskem sistemi sestavljen iz jedrne aplikacije IBIS++ ter spletnega portala, poimenovanega portal OT (v nadaljevanju tudi: portal). V obstoječi informacijski rešitvi so bila zaznana določena varnostna tveganja in tehnološka zastarelost, kar ob povečevanju kompleksnosti trga in količine podatkov (15-minutni obračunski interval, večje prevzemno predajnih mest itd.) predstavlja tveganje za operativno delovanje. Projekt prenove informacijskega sistema (v nadaljevanju: IBIS++) je usmerjen v celovito tehnološko posodobitev in odpravo varnostnih ranljivosti, hkrati pa v ohranitev in nadgradnjo vseh ključnih funkcionalnosti trenutne rešitve.

Z novo rešitvijo bo naročnik dosegel višjo stopnjo kibernetske varnosti, boljšo odzivnost sistema pri obdelavi velikih količin podatkov ter zagotovil skladnost z najnovejšimi standardi informacijske varnosti. Prenova je strateškega pomena, saj Borzenu omogoča nemoteno izvajanje javnih pooblastil, ohranjanje zaupanja regulatorjev (Agencija za energijo) ter vseh udeležencev na trgu z elektriko.

Namen dokumenta je opredeliti tehnične zahteve za prenovo informacijske rešitve IBIS++/OT portal.

Prenova obsega migracijo AngularJS modulov na sodoben Angular ter prenovo UX/UI. Široko uporabljano še vzdrževano tehnologijo, za katero razvijalec platforme še zagotavlja podporo. Izvajalec mora prav tako predlagati optimalno tehnologijo za osnovno platformo za OT portal (naročnik uporablja DNN ali, vendar lahko izvajalec predlaga alternativno tehnologijo v okviru naročnikovega tehničnega portfelja). Dokument definira obseg, funkcionalnosti, varnostne zahteve, arhitekturo, testiranja ter zahteve za vzdrževanje in prevzem.

1.2. Umestitev projekta v širše okolje naročnika

V okviru projekta je zastavljena obsežna prenova sistema IBIS++ in spletnega portala OT znotraj celotnega ekosistema Borzenovih informacijskih rešitev. Nova rešitev bo služila kot osrednje

vozlišče za izvajanje bilančnega obračuna, poročanje o tržnih podatkih ter interakcijo s člani bilančne sheme. Naslovila bo nove zahteve, ki jih prinaša posodobljena energetska regulativa in naraščajoče potrebe po varnem zbiranju in obdelavi merilnih podatkov.

Pri načrtovanju nove rešitve je poudarjena integracija z obstoječimi storitvami in zunanjimi sistemi operaterjev (ELES, Informatika). Sistem IBIS++ bo tesno povezan z naročnikovim centralnim registrom matičnih podatkov (MDM) in drugimi ključnimi sistemi:

Integracija z ERP sistemom (npr. SAOP): Za avtomatski prenos podatkov za fakturiranje bilančnega obračuna, uvoz podatkov o finančnih kritjih in izmenjavo finančnih izpiskov.

Povezava z zunanjimi platformami: Izmenjava podatkov po mednarodnih standardih oz. usklajenimi načini izmenjave podatkov (CEEPS).

Portal OT kot vstopna točka: Portal bo ostal ključni vmesnik za zunanje uporabnike (člane bilančnih skupin, operaterje), ki bo omogočal varno prijavo preko 2FA, oddajo vlog za vstop v shemo, pregled rezultatov obračuna, vlaganje pripomb ipd.

Ključna usmeritev projekta je, da nova rešitev IBIS++ nadomesti trenutno tehnološko osnovo (.NET 4.5.1, AngularJS), pri čemer ne posega v uveljavljeno poslovno logiko, ki se je izkazala za ustrezno, temveč jo optimizira za delovanje v sodobnem in varnem okolju. Sistem bo že v prvi fazi v celoti integriran s sistemom za upravljanje uporabnikov (Active Directory / Entra ID) za enotno prijavo (SSO) in granularno upravljanje dostopnih pravic.

IBIS++ mora biti skladen z zahtevami varstva osebnih podatkov (GDPR/ZVOP-2) ter zagotavljati visoko stopnjo kibernetске varnosti skladno z direktivo NIS2 in Zakonom o informacijski varnosti, saj Borzen upravlja s podatki, ki so kritični za energetski sektor. Rešitev bo podpirala načela sistemov vodenja kakovosti ISO 9001 in informacijske varnosti ISO 27001, ki sta že vpeljana v družbi, s čimer se zagotovi celostna skladnost poslovanja na enem mestu.

1.3. Glavne faze implementacije projekta

Projekt se izvede fazno. V fazi analize se pripravi podroben načrt izvedbe, migracije in testiranja, vključno z merili sprejema za posamezne funkcionalne in nefunkcionalne zahteve. Faze izvedbe in ključni mejniki so opisani v nadaljevanju dokumenta (poglavje »Načrt implementacija in vzdrževanje«).

2. Strateški okvir

Borzen, kot operater trga z elektriko v Sloveniji, deluje v okolju strogih in dinamičnih regulatornih zahtev, hkrati pa upravlja s kritičnimi podatki, ki so podlaga za finančno poravnavo celotnega elektroenergetskega sistema. V tem kontekstu je prenova jedrne aplikacije za bilančni obračun (IBIS) in portala za udeležence trga (Portal OT) strateškega pomena za družbo.

S prenovo se bo odpravilo zaznana varnostna tveganja, izboljšalo odzivnost sistema, optimiziralo obstoječe delovanje ter nadgradilo funkcionalnosti sistema. Projekt tako ni le tehnična nadgradnja zastarele tehnologije, temveč strateška naložba v stabilnost energetskega

trga, ki neposredno podpira ključne poslovne cilje družbe (natančnost, kibernetska odpornost, operativna odličnost) in jih povezuje s širšo digitalno preobrazbo podjetja.

2.1. Strateški cilji

Strateški cilj	Opis cilja
Operativna odličnost in stabilnost trga	Doseganje zanesljivega izvajanja bilančnega obračuna kot temeljne dejavnosti operaterja trga. IBIS++ bo k temu prispeval z optimiziranimi algoritmi, krajšimi časi obdelave in zmanjšanjem ročnih korekcij.
Digitalizacija in avtomatizacija podatkovnih tokov	Standardizacija izmenjave podatkov z elektrooperaterji (ELES, Informatika), regulatorjem in člani bilančne sheme. Nova rešitev neposredno udejanja ta cilj z nadgradnjo izmenjave podatkov ter z digitalizacijo oddaje vlog za vstop v bilančno shemo.
Kibernetska varnost in skladnost	Zagotavljanje najvišje stopnje zaščite kritične energetske infrastrukture. Z odpravo varnostnih ranljivosti in skladnostjo z direktivo NIS2 ter standardom ISO 27001 bo Borzen lažje obvladoval tveganja in ščitil občutljive podatke.

2.2. Poslovni cilji

Poslovni cilji projekta IBIS++ izhajajo iz konkretnih potreb po prenovi trenutno zastarele rešitve in pričakovanih koristi za udeležence trga. Projekt bo prinesel izboljšave, ki bodo povečale zanesljivosti in zaupanje v rezultate BO ter zagotavljale transparentnost:

Poslovni cilj projekta IBIS++	Opis poslovnega cilja	Povezava s strateškimi cilji
Odprava varnostnih tveganj	Prehod na sodobno in podprto tehnološko platformo, ki bo odpravila varnostne vrzeli trenutne rešitve in omogočila dolgoročno vzdrževanje sistema.	Kibernetska varnost in skladnost
Natančnost in hitrost bilančnega obračuna	Skrajšanje časa potrebnega za izvedbo BO in LPBO ob zagotavljanju zanesljivosti in natančnosti izračunov po pravilih trga.	Operativna odličnost
Izboljšana uporabniška izkušnja na Portalu OT	Ponuditi članom bilančne sheme sodoben, pregleden in varen portal za spremljanje podatkov trga, postopkov BO, oddajo pripomb in vpogled v finančna kritja.	Digitalizacija procesov

Posodobitev procesov izmenjave podatkov z zunanjimi deležniki	Vzpostavitev posodobljenih izmenjav podatkov s CEEPS, ELES ter Agencijo za povečanje varnosti in zanesljivosti teh procesov.	Operativna odličnost; Inovativnost
Nadgradnje in avtomatizacije integracij v naročnikovem okolju	Optimizacija obstoječih integracijskih postopkov bo omogočila manj ročnih posegov in s tem možnost napak.	Operativna odličnost; Digitalizacija

2.3. Tehnični cilji

Za uspešno uresničitev poslovnih ciljev mora projekt izpolniti jasne tehnične cilje, ki opredeljujejo zmogljivosti nove rešitve IBIS++:

Tehnični cilj	Opis tehničnega cilja	Povezava s strateškimi cilji
Sodobna arhitektura in skalabilnost	Vzpostaviti sistem na tehnologijah .NET 8+ (ali enakovredno) z ločenim front-end in back-end delom, ki omogoča procesiranje več velikih količin podatkov.	Operativna odličnost; Digitalizacija
Varno upravljanje identitet in dostopov	Integracija z Microsoft Entra ID (Active Directory) za enotno prijavo (SSO) in uporaba naprednih metod avtentikacije za zunanje uporabnike.	Kibernetska varnost
Robusten motor za izračune (Calculation Engine)	Vzpostaviti motor za izračune, ki omogoča hitro in zanesljivo izračunavanje BO in LPBO ter ostale operacije/algoritme znotraj aplikacije.	Operativna odličnost
Napredna revizijska sled in celovitost podatkov	Implementirati nespremenljivo revizijsko sled (Audit Trail) za vsako spremembo v podatkih ali algoritmih, kar zagotavlja dokazljivost rezultatov obračuna v primeru sporov.	Skladnost poslovanja; Varnost
Visoka razpoložljivost in načrt okrevanja (DRP)	Arhitektura sistema mora podpirati delovanje v visoko razpoložljivem načinu (High Availability) s hitrim časom okrevanja v primeru tehničnih težav.	Operativna odličnost; Varnost

2.4. Regulatorni okvir in standardi

2.4.1. Energetski in sektorski pravni okvir

Prenova sistema IBIS++ mora v celoti slediti specifični področni zakonodaji, ki ureja trg z električno energijo in vlogo naročnika kot operaterja trga. Ključni stebri so:

Pravila za delovanje trga z elektriko: Ta podzakonski akt natančno določa postopke (algoritme) in roke bilančnega obračuna, vključno z metodologijo za izračun odstopanj in cen. Rešitev IBIS++ mora omogočati 100-odstotno skladnost s temi pravili.

Energetski zakon (EZ-2): Kot temeljni predpis določa okvir delovanja energetskega sektorja, vlogo naročnika ter obveznosti glede preglednosti in zanesljivosti podatkov.

Zakon o oskrbi z električno energijo (ZOOE): Podrobneje ureja dejavnost operaterja trga, organizacijo bilančne sheme in izvajanje bilančnega obračuna, kar mora IBIS++ neposredno tehnično podpirati.

Obratovalna navodila systemskega operaterja: Sistem mora omogočati izmenjavo podatkov z operaterji (ELES, EDP, ZDS) v skladu z veljavnimi pravili o izmenjavi podatkov na slovenskem trgu.

2.4.2. Splošni slovenski pravni okvir

Poleg sektorskih predpisov mora rešitev izpolnjevati horizontalne zahteve slovenske zakonodaje:

Zakon o informacijski varnosti (NIS2 oz. ZInfV-1): Borzen je zavezanec kot izvajalec bistvenih storitev v energetiki. IBIS++ mora izpolnjevati stroge tehnične zahteve za varnost omrežij in informacijskih sistemov.

Zakon o varstvu osebnih podatkov (ZVOP-2) in GDPR: Sistem bo obdeloval podatke kontaktnih oseb članov bilančne sheme in morebitne podatke o merilnih mestih fizičnih oseb (npr. samooskrba), zato mora podpirati načela "privacy by design" in zagotavljati revizijsko sled obdelav.

Zakon o elektronski identifikaciji in storitvah zaupanja (ZEISZ): Ureja postopke za dostop do portala OT in e-podpisovanje pogodb ali poročil v delih, ki jih ne ureje eIDAS.

Zakon o javnem naročanju (ZJN-3): Ker je naročnik zavezanec za javno naročanje, mora biti rešitev pripravljena tako, da ne povzroča t.i. "vendor lock-in" situacije in temelji na standardnih vmesnikih.

2.4.3. Zakonodaja in kodeksi Evropske unije

Kot operater trga v povezanem evropskem sistemu mora Borzen zagotoviti, da IBIS++ podpira zahteve evropskih mrežnih kodeksov, smernic in direktiv:

ENTSO-E mrežni kodeksi in smernice:

EBGL (Electricity Balancing Guideline): Uredba (EU) 2017/2195 o smernicah za bilančno obdelavo električne energije. IBIS++ mora podpirati procese poravnave odstopanj, ki so usklajeni s tem kodeksom.

CACM (Capacity Allocation and Congestion Management): Uredba (EU) 2015/1222 o določitvi smernic za dodeljevanje zmogljivosti in upravljanje s preobremenitvami, ki vpliva na tržne plane in obračune.

Kodeks za fleksibilnost (v pripravi): Arhitektura sistema mora biti zasnovana modularno, da bo omogočala prihodnjo integracijo zahtev glede storitev prilagajanja odjema in fleksibilnosti.

Direktiva (EU) 2022/2555 (NIS2): Nova direktiva o kibernetiski varnosti, ki od Borzena zahteva vzpostavitev najvišjih varnostnih ukrepov, upravljanje tveganj v dobavni verigi in hitro odzivanje na incidente v sistemu IBIS++.

Uredba eIDAS: Zagotavljanje čezmejne interoperabilnosti elektronskih podpisov in identifikacije za tuje člane bilančne sheme.

2.4.4. Standardi in dobre prakse

Naročnik že deluje v skladu z uveljavljenimi standardi, ki jih mora nova rešitev IBIS++ aktivno podpirati:

ISO/IEC 27001 (Informacijska varnost): Naročnik ima certifikat, zato mora IBIS++ vključevati kontrole, kot so granularno upravljanje dostopov, šifriranje podatkov in dnevniki dogodkov.

ISO 9001 (Vodenje kakovosti): Dokumentiran razvoj, testiranje in vzdrževanje sistema v skladu s procesi naročnika.

ENTSO-E in CIM standardi: Za izmenjavo podatkov med udeleženci trga mora sistem podpirati standardizirane XML/JSON sheme in protokole (npr. MADES/AS4, če relevantno), ki jih predpisujejo evropska združenja.

ITIL smernice: Za operativno podporo uporabnikom portala OT in vzdrževanje zalednega sistema IBIS++.

2.4.5. Zagotavljanje skladnosti pri implementaciji IBIS++

Skladnost s predpisi mora biti integrirana v vse faze razvoja:

Analiza algoritmov: Ponudnik mora skupaj z naročnikom preveriti, ali matematični modeli v kodi IBIS++ natančno odražajo zahteve iz Pravil za delovanje trga.

Varnostno načrtovanje (Security by Design): Implementacija zaščite pred napadi (OWASP Top 10) in varna avtentikacija zunanjih uporabnikov preko Portala OT.

Sledenje in revizija: Sistem mora omogočiti rekonstrukcijo katerega koli obračuna za nazaj (npr. v primeru nadzora Agencije za energijo) z vpogledom v takrat veljavne vhodne podatke in parametre.

Testiranje skladnosti: Pred prehodom na produkcijo se izvedejo testi, ki potrdijo pravilnost izračunov na testnih scenarijih, ki vključujejo mejne primere (npr. negativne cene, izredni dogodki v sistemu).

Interoperabilnost: Potrditev uspešne izmenjave podatkov z zunanjimi sistemi (EIP - CEEPS, ELES, Agencija) po predpisanih standardih.

3. Poslovne zahteve

Prenova mora ohraniti funkcionalnosti trenutnega sistema, ki so navedene v nadaljevanju. V primeru, da določena funkcionalnost trenutnega sistema ni zavedena na spodnjem seznamu, je izvajalec v sklopu projekta dolžan z naročnikom dogovoriti, če se funkcionalnost ohrani ali ne ohrani. Trenutna rešitev podpira naslednje glavne naloge, ki so podrobneje opisane v nadaljevanju specifikacije:

Portal OT

- a. objava bistvenih podatkov trga za namen preglednosti trga z elektriko - tako avtomatska (viri DWh in aplikacija IBIS++) kot ročna,
- b. vodenje bilančne sheme (sprejem novih članov, dostop do dokumentov glede članstva, finančni dokumenti in obvestila, spremembe podatkov članov - pooblaščen uporabniki, kontaktni podatki),
- c. posredovanje rezultatov BO in LPBO članom trga z dostopom do portala,
- d. vodenje celotnega postopka BO in LPBO (npr. pripombe) in
- e. upravljanje uporabnikov portala,
- f. upravljanje lastnih nastavitev (opomnik).

Aplikacija za bilančni obračun (Aplikacija IBIS++):

- a. prejem podatkov od elektrooperaterjev,
- b. upravljanje in urejanje osnovnih podatkov partnerjev ter kontaktnih oseb,
- c. izračun bilančnega obračuna (nastavitve, izračuni),
- d. izračun letnega poročila bilančnega obračuna,
- e. priprava rezultatov BO in LPBO za člane trga (poročila, podatki),
- f. analitika podatkov BO in LPBO ter prikaz bistvenih podatkov in izvoz v uporabne oblike dokumentov.

3.1. Funkcionalne zahteve (FR) OT portala

ID	Zahteva	Prioriteta	Povzetek	Preverjanje
FR-OT-001	Javni del portala	OBVEZNO	Javni del portala mora ohraniti vse obstoječe vsebinske in funkcionalne sklope ter omogočati objavo vsebin in dokumentov.	Funkcionalni test + pregled

FR-OT-002	Splošno	OBVEZNO	Portal mora ohraniti obstoječe splošne zmožnosti (npr. struktura strani, objava dokumentov, osnovna navigacija) in podpreti migracijo brez izgube funkcionalnosti.	Pregled + SAT
FR-OT-003	Javni del portala - Podatki trga	OBVEZNO	Javni prikaz podatkov trga (grafi, tabele, datoteke) se ohrani; podatki se prikazujejo v enaki ali izboljšani obliki kot v obstoječi rešitvi.	Funkcionalni test
FR-OT-004	Uporabniški del portala - splošno	OBVEZNO	Zasebni del portala mora omogočati varno delo registriranih uporabnikov ter dostop do dokumentov, finančnih podatkov in obračunov glede na pravice.	SAT
FR-OT-005	Uporabniški del portala - spletne vloge/obrazci za	OBVEZNO	Podprti morajo biti opisani spletni obrazci/vloge	Funkcionalni test + SAT

	vstop v bilančno shemo		(OBS/OBPS ipd.) s prilagojenimi delovnimi tokovi, validacijami in statusi.	
FR-OT-006	Registracija in prijava uporabnika	OBVEZNO	Zagotoviti je treba varen postopek registracije in prijave (z MFA za zunanje uporabnike, SSO za interne) ter povezavo z MDM za dodeljevanje pravic.	Varnostni + funkcionalni test
FR-OT-007	Ponastavitev gesla	OBVEZNO	Uporabnik mora imeti varen postopek ponastavitve gesla ter upravljanje ponastavitve drugega faktorja skladno z varnostnimi politikami.	Funkcionalni test
FR-OT-008	Ravni pravic in upravljanje z uporabniki	OBVEZNO	Upravljanje uporabnikov in vlog (RBAC) mora omogočati dodeljevanje pravic po članih BS/BPS ter revizijsko sled sprememb pravic.	Pregled + funkcionalni test

FR-OT-009	Vloge/zahteve znotraj portala	OBVEZNO	Portal mora podpirati oddajo, obdelavo in pregled poslovnih zahtev (vlog) z definiranimi statusi, komentarji in pravili prehodov.	Funkcionalni test
FR-OT-010	Struktura Menu-ja portala OT	OBVEZNO	Struktura menija in navigacije se ohrani; prehodi med sklopi morajo biti uporabniku pregledni in konsistentni.	Pregled
FR-OT-011	Novice in obvestila	OBVEZNO	Portal mora omogočati objavo novic in obvestil (kategorizacija, arhiv, prikaz na javnem in/ali zasebnem delu).	Pregled funkcionalni test +
FR-OT-012	Pregled dokumentov bilančne sheme	OBVEZNO	Uporabnikom se zagotovi pregled in prenos dokumentov bilančne sheme glede na pravice; podprto je verzioniranjem in metapodatki dokumentov.	Funkcionalni test

FR-OT-013	Prikaz, pregled finančnih podatkov	OBVEZNO	Portal mora prikazovati ključne finančne podatke (kritja, obračuni, dokumenti) in omogočati izvoz/prenos, kot v obstoječi rešitvi.	SAT
FR-OT-014	Podatki o bilančnih obračunih in letnih poračunih bilančnega obračuna	OBVEZNO	Portal mora omogočati dostop do podatkov in poročil za BO in LPBO ter pregled statusov in rokov.	SAT
FR-OT-015	Upravljanje s pripombami na BO	OBVEZNO	Uporabnikom je treba omogočiti oddajo pripomb na BO v definiranih rokih, pregled obdelave in zgodovino komunikacije.	Funkcionalni test
FR-OT-016	Obveščanja in naročilo na obveščanja	OBVEZNO	Portal mora podpirati naročnine na obveščanja (e-pošta) ter upravljanje predlog in čakalnih vrst pošiljanja.	Funkcionalni test
FR-OT-017	Administratorski (skrbniški) del portala	OBVEZNO	Skrbniški del mora omogočati upravljanje vsebin,	SAT + pregled

			uporabnikov, vlog, dokumentov in nastavitev ter zagotavljati revizijsko sled.	
FR-OT-018	Dodajanje, registracija in prijava administratorja	OBVEZNO	Postopki dodeljevanja skrbniških pravic in prijave skrbnikov morajo biti varni, sledljivi in usklajeni z IAM politikami naročnika.	Pregled + varnostni test
FR-OT-019	Urejanje vlog	OBVEZNO	Skrbnik mora imeti možnost pregleda in obdelave vseh vrst vlog ter urejanja nastavitev, povezanih z delovnimi tokovi.	Funkcionalni test
FR-OT-020	Urejanje in sinhronizacija kontaktov (kontaktnih oseb)	OBVEZNO	Sinhronizacija kontaktov z MDM (MDM → portal) in prenos sprememb prek vlog (portal → MDM) se ohrani; definira se pravila in urnike.	Integracijski test
FR-OT-021	Urejanje dokumentov	OBVEZNO	Skrbnik upravlja dokumente (kategorije, metapodatki,	Funkcionalni test

			vidnost) in sinhronizacijo z zunanjsimi repozitoriji skladno z obstoječim procesom.	
FR-OT-022	Nastavitve opomnikov in obvestil	OBVEZNO	Skrbnik ureja opomnike in predloge obvestil, pregleda zgodovino pošiljanja ter upravlja čakalno vrsto.	Funkcionalni test
FR-OT-023	Beleženje dostopa do datotek	OBVEZNO	Sistem mora beležiti dostop do dokumentov in prenosov (kdo, kdaj, kaj) ter omogočiti skrbniški pregled in izvoz.	Pregled + test

Portal OT je namenjen javnem prikazu informacij o delovanju trga z električno energijo, ter članom bilančne sheme, prednostno za potrebe procesa bilančnega obračuna, hkrati pa tudi upravljanja ostalih podatkov, ki so pomembni z vidika članstva v bilančni shemi. Portal je razdeljen na javni in zasebni del. Javni del je dostopen vsem, zasebni pa registriranim uporabnikom.

Dostop do javnega dela ni omejen (je javen, kot spletna stran), zasebni del portala pa je razdeljen na različne ravni pravic, ki jih bodo imeli posamezni uporabniki.

Portal omogoča objavo dokumentov, na primer v obliki .xlsx, .pdf, .csv, .xml, .docx tako na javnem kot zasebnem delu.

Portal je trenutno baziran na rešitvi Dot Net Nuke, ki združuje funkcionalnosti za:

- grafično urejanje portala,
- upravljanje z meniji in vsebino portala,

- upravljanje z uporabniki ter pravicami dostopa,
- podpora večjezičnosti,
- upravljanje z dokumenti na javnem delu portala,
- itd.

Portal je grajen na način, da se lahko v spletne strani vključi različna orodja v obliki modulov, ki se jih namesti v okvirju administracije portala. Portal torej omogoča razširljivost vsebine ter implementacijo standardnih modulov, ki so grajeni s strani tretjih oseb.

Osnovni pristop pri zasnovi mora zagotoviti, da se uporabijo prilagoditvene zmožnosti (resolucija, mobilne naprave). Morebitne problematične elemente se po dogovoru lahko pri določenih prikazih omeji, spremeni ali odstrani. Pri oblikovanju se upošteva CGP Borzen, oblikovalske zasnove se sproti usklajujejo z naročnikom.

3.1.1. Javni del portala

3.1.1.1. Splošno

Dostop do javnega dela portala imajo vsi obiskovalci portala. Namen tega je prikaz novic operaterja trga, raznih informacij ter povezav v zvezi s trgov z električno energijo in bilančnim obračunom, navodil za registracijo oziroma pristop bilančnih skupin in podskupin ter prikaza informacij, podatkov ter analiz za transparenten pregled delovanja trga.

Poleg javnih vsebin so na portalu na voljo tudi forme, s katerimi se izpolni vloge za pridobitev statusa odgovornega bilančne skupine (OBS) in odgovornega bilančne podskupine (OBPS).

Upravljanje z javnim delom portala je izvedeno tako, da skrbnik portala ureja, dodaja ali briše javne menijske vrstice, ter za vsakega izmed teh definira vsebino. Del vsebine bo popolnoma prilagodljiv, del vsebine pa bo izveden v sklopu razvoja. Del portala ne bo mogoče spreminjati ali urejati brez posega razvijalca/izvajalca, kar se določi v okviru projekta.

Kompatibilnost URL in preusmeritve: Pri prenovi portala se morajo ohraniti obstoječe povezave (URL) javnega dela portala. Če zaradi menjave CMS ali strukture strani ohranitev ni možna, mora izvajalec vzpostaviti trajne preusmeritve (HTTP 301) z obstoječih URL na nove URL. Seznam kritičnih URL in pravila preusmeritev se potrdi z naročnikom v fazi analize; preusmeritve se preverijo pred produkcijskim preklpom.

3.1.1.2. Javni del portala - Podatki trga

Modul za zagotavljanje urejenega in preglednega trga z elektriko zajema prikaze grafov, tabel in datotek, ki vsebujejo podatke trga. Vsak sklop podatkov bo prikazan v ločeni menijski vrstici oziroma pod-vrstici. Modul mora omogočiti prikaze in z njimi povezane funkcionalnosti (filtriranje, sortiranje, agregiranje, izvoz podatkov, izbor seriji itd.) najmanj na način, kot je to omogočeno na trenutnem portalu na naslednjih povezavah:

<https://ot.borzen.si/Domov/Podatki-trga/Cene-odstopani>

<https://ot.borzen.si/Domov/Podatki-trga/Koli%C4%8Dine-in-zneski-izravnave>

<https://ot.borzen.si/Domov/Podatki-trga/Preostali-diagram-odjema>

<https://ot.borzen.si/Domov/Podatki-trga/Dobavitelji>
<https://ot.borzen.si/Domov/Podatki-trga/Bilan%C4%8Dna-shema>
<https://ot.borzen.si/Domov/Podatki-trga/Indeks-izravnalnega-trga>
<https://ot.borzen.si/Domov/Podatki-trga/Podatki-o-izravnalnem-trgu>
<https://ot.borzen.si/Domov/Podatki-trga/%C4%8Clani-izravnalnega-trga>
<https://ot.borzen.si/Domov/Podatki-trga/Vrednostni-pregled-bilan%C4%8Dnega-obra%C4%8Duna>
<https://ot.borzen.si/Domov/Podatki-trga/Napoved-proizvodnje-in-odjema>
<https://ot.borzen.si/Domov/Podatki-trga/Koeficient-izgub>

Prednastavljeni prikazi se prevzamejo iz objav iz trenutne rešitve.

3.1.2. Uporabniški del portala - splošno

Zasebni oz. uporabniški del portala je namenjen registriranim uporabnikom bilančnih skupin, podskupin ter ostalim udeležencem trga. Prijava v zasebni del portala je mogoča preko 2FA s pomočjo mobilne aplikacije MS Authenticator. Način implementacije dvofaktorske avtentikacije in administracije uporabnikov se uskladi v sklopu projekta.

Skozi celoten uporabniški del portala se zagotovi, da je vse prikaze v tabelah mogoče filtrirati in razvrščati na podlagi prikazanih podatkov, parametrov. Pri vseh tabelah mora biti prisotna možnost izvoza podatkov v standardnih podatkovnih formatih (csv, xlsx, xml ipd.). Portal mora funkcionalnosti iz tega odstavka omogočati najmanj na način, ki je podprt v trenutnem portalu.

3.1.2.1. Uporabniški del portala - spletne vloge/obrazci za vstop v bilančno shemo

Vzpostavi se prenovljen digitaliziran obrazec za vlogo za OBS in OBPS ter vzpostavi sistem spremljanja statusa vloge, ki je neposredno povezan v zaledne sisteme naročnika.

Za izpolnjevanje obrazcev se bo po novem potrebno predhodno registrirati v portal. Podatke, ki bodo potrebni ob registraciji se dorečejo z naročnikom v sklopu projekta. Profil takega uporabnika bo omogočal le pravice in vpogled do vnosnih obrazcev ter s tem procesom povezanih podatkov. Preko tega uporabniškega profila se lahko vnaša vloge, spremlja status obdelav vlog, nalaga in pregleduje naložene dokumente, ureja lastne nastavitve ipd. V nadaljevanju se temu uporabniku, če podjetje uspešno pridobi status OBS/OBPS, dodeli tudi dodatne pravice znotraj portala - skladno s prejeto vlogo za OBS/OBPS.

Trenutna digitalna obrazca se nahajata na spodnji povezavi:

[OBS](#)
[OBPS](#)

Vsebina trenutnih spletnih obrazcev ter način izvedbe (kot čarovnik za izpolnjevanje, kjer je v določenem pogledu na voljo le določen (omejen) nabor vnosnih polj) se ohrani. Obrazci morajo omogočati dodajanje/urejanje pomoči/tooltipov pri posameznih poljih. Vzpostavi se validacije za vnos v posamezna polja (ohrani se obstoječe validacije, pri določenih poljih se slednje lahko prilagodijo). Validacije so avtomatske in sprotne. Če je vnos nepravilen se polje označi in

opozori na napako oz. prikaže primer pravilne izpolnitve polja. S potrditvenim gumbom potrdi vnesene podatke ter se premakne na naslednjo stran. Uporabnik se lahko v tem pomakne tudi nazaj na predhodni oz. predhodne preglede in po potrebi popravi vnesene podatke.

Po zaključku vnosa in potrditvi obrazca se generira PDF vloge, ki vsebuje predhodno vnesene podatke. Za zaključek postopka se uporabnik pomakne na zadnjo stran obrazca, kjer naloži priloge. Uporabnik mora imeti možnost naložiti več datotek različnih tipov (npr. ID za DDV, izpis iz sodnega registra ipd.), pri čemer mora biti vsak dokument vsebinsko razločen (izbor tipa dokumenta). Poleg ostalih dokazil uporabnik naloži tudi PDF vloge, ki mora biti digitalno podpisane (s strani zakonitega zastopnika ali pooblaščenca). Če zahtevani dokumenti niso naloženi, obrazec ne dovoli končne oddaje vloge. Skrbnik mora imeti možnost urejanja seznama obveznih tipov dokumentov (dodajanje, brisanje, sprememba oznake/poimenovanja).

Preverjanje digitalnega podpisa: Pred končno oddajo mora portal izvesti avtomatsko preverjanje, ali je naloženi PDF podpisan in ali je podpis tehnično veljaven (npr. PAdES). Rezultat preverjanja (veljaven/neveljaven/nepreverljiv) se zabeleži in je viden v skrbniškem vmesniku pri obdelavi vloge.

Podatki o podpisu: Sistem mora hraniti najmanj: identiteto podpisnika (če je razvidna iz potrdila), izdajatelja potrdila, čas podpisa oziroma časovni žig (če je prisoten), ter kriptografski povzetek (hash) dokumenta. Namen je dokazljivost in revizijska sled.

Ravnanje ob napakah: Če je podpis neveljaven ali manjkajoč, portal uporabniku prikaže razumljivo sporočilo z navodili za odpravo težave in ne dovoli oddaje vloge.

Vse dokumente, ki se naloži in izmenjuje preko portala, je potrebno opremiti z metapodatki, ki se jih določi z naročnikom, ter zagotovi prenos v zaledne sisteme naročnika (DMS, EIS). Hkrati je potrebno v zaledne sisteme avtomatsko prenesti tudi ostale podatke, ki jih uporabnik vnesel v (uspešno) oddano vlogo, kar se uskladi z naročnikom.

V administratorskem delu portala se vzpostavi sistem za upravljanje notranjega delovnega procesa pregleda vlog. Preko svojih uporabniških profilov bodo vključeni interni deležniki/zaposleni, ki bodo imeli možnost pregleda, potrditve, zavrnitve oz. vnosa zahteve za dopolnitev, ki bo nato preko skrbnika procesa poslana zunanjemu uporabniku / vlagatelju; ta informacija pa bo dostopna tudi znotraj uporabniškega računa vlagatelja.

Vzpostavi se funkcionalnost, ki skrbnikom/administratorjem omogoča spremljanje posamezni korakov pri obdelavi vlog (datum oddaje, pozivi za dopolnitev, opomniki, število dni med dejavnostmi) na način, da je možen pregled trajanja posameznih korakov procesa. Vzpostavi se tudi pregled oz. poročilo, ki prikazuje časovno os in trajanja posameznih korakov tako na ravni posameznega partnerja kot tudi povprečji za izbrana obdobja.

Vzpostavi se tudi sistem opomnikov za opozarjanje na potrebne aktivnosti. Opomnik se lahko nanašajo na interne ali zunanje naloge uporabnikov. Za nastavitve opomnikov (besedila, časovni parametri) se vzpostavi ločen modul.

Vzpostaviti je potrebno klepetalnik »chatbot«, ki je na voljo uporabniku pri izpolnjevanju vloge in mu pomaga z informacijami in odgovori na vprašanja, pri čemer pa gre zgolj za integracijo z naročnikovo infrastrukturo za klepetalnike; vzpostavitev infrastrukture ni predmet tega projekta.

Klepetalnik je informativne narave in ne sme ustvarjati pravno ali poslovno zavezujočih odločitev. Uporabniku mora jasno prikazati, da gre za podporno orodje in ponuditi povezavo na uradna navodila oziroma kontaktno točko za pomoč.

Rešitev mora vključevati zaščito pred zlorabami (npr. omejevanje zahtevkov, filtriranje škodljivih vsebin, zaščita pred prompt-injection pri uporabi LLM) ter možnost popolnega izklopa klepetalnika brez vpliva na ostale funkcionalnosti portala.

Interakcije se beležijo v obsegu, ki je potreben za izboljšave in varnostni nadzor (npr. metapodatki in anonimizirani vnosi), s politiko hrambe, določeno z naročnikom.

3.1.2.2. Registracija in prijava uporabnika

V obstoječem Portalu OT je bil za dostop v uporabniški del zahtevan dostop z digitalnim potrdilom. V prenovljenem Portalu OT digitalna potrdila niso več pogoj za prijavo. Preverjanje pristnosti se izvede z uporabniškim imenom in geslom ter z dodatnim dejavnikom (2FA/MFA) za zunanje uporabnike. Za interne uporabnike naročnika (zaposlene) se praviloma uporabi enotna prijava (SSO) prek identitetnega ponudnika (npr. Microsoft Entra ID) v skladu z internimi politikami naročnika.

Registracija uporabnikov bo potekala na naslednje načine:

- Registracija preko obrazca na javnem delu portala (za tiste, ki želijo izpolniti vlogo za OBS/OBPS),
- Registracijo sproži admin na podlagi popolne vloge za OBS/OBPS,
- Registracijo sproži obstoječi uporabnik znotraj uporabniškega dela portala,
- Registracijo internih (admin) uporabnikov sproži admin.

Ob registraciji se zunanji uporabnik v izbrani mobilni aplikacija (denimo MSaplikaciji (npr. Microsoft Authenticator) ustvarivzpostavi račun za izvajanje 2FA. Postopek namestitve aplikacije, dodajanja račun v tej aplikaciji in vse podrobnosti za zaključek postopkaračuna in zaključka registracije se uskladi z naročnikom v okviru projekta. V procesu registracije si uporabnik Uporabnik si nastavi geslo, ki mora ustrezati varnostnim politikam podjetja. naročnika (minimalna dolžina, kompleksnost, zgodovina gesel ipd.). Portal zavrne registracijo prekratkega oz. neustreznega gesla ter vodi prekratko oziroma neustrezno geslo ter uporabnika, da ustvari geslo, ki je vodi k nastavitvi ustrezno kompleksno. kompleksnega gesla.

Administracija uporabnikov poteka preko portalaprek Portala OT. Vse obstoječe delovne tokove znotraj trenutnega portala, ki se jih uporablja za upravljanje uporabnikov, se prilagodi tako, da se odstrani vse, kar se nanaša na , ki so povezani z uporabo digitalnih potrdil (pojavnostiprikazi na vmesniku, vloge in delovne tokove, ki so povezani z digitalnimi potrdili, ki

jih v prenovljeni aplikacijodobritve), se prilagodi tako, da se odstrani odvisnost od digitalnih potrdil in portalu nadomeščamo z uvede 2FA). Doda se /SSO. Skrbnik mora imeti možnost, da skrbnik/administrator upravlja možnosti upravljanja nastavitvev 2FA pri posameznih uporabnikih (preklic na neki napravi, vzpostavitev na novi ipd.).

Prijava za posameznega uporabnika je mogoča ob predhodno izvedeni uspešni registraciji uporabnika. Uporabnik mora vnesti uporabniško ime in geslo. Na tem mestu je na razpolago možnost za ponastavitev gesla. Ob ustreznem vnosu gesla uporabnik v naslednjem koraku preko izbrane mobilne aplikacije za 2FA potrdi svojo identiteto. Tukaj je dodana možnost ponovne vzpostavitve računa za 2FA za primere, ko uporabnik zamenja mobilno napravo ali je iz katerega drugega razlog smiselno ponastaviti račun(npr. ponastavitev drugega faktorja, preklic zaupanja za izgubljeno napravo, dodajanje nove naprave), pri čemer mora biti vsak poseg revizijsko sledljiv.

Prijava je mogoča po uspešno zaključeni registraciji uporabnika. Zunanji uporabnik se prijavi z uporabniškim imenom (praviloma e-poštni naslov) in geslom, nato pa svojo identiteto potrdi z 2FA. Interni uporabnik se prijavi prek SSO (npr. Entra ID); dodatni faktor se uveljavlja skladno s politikami pogojnega dostopa naročnika. Sistem mora podpirati tudi ponastavitev 2FA (npr. ob menjavi naprave) po nadzorovanem postopku.

Vsak uporabniški račun na portalu mora biti vezan na ustrezen zapis kontaktne osebe v MDM (MDM ContactID). Dodeljevanje pravic in pripadnosti podjetju (partnerju) se izvaja na podlagi podatkov v MDM (npr. isPortalUser, vloge kontaktne osebe, aktivnost kontakta).

Uporabniško ime (e-poštni naslov) mora biti enolično. Sistem mora preprečiti dvojne registracije za isto kontaktno osebo ter zagotoviti kontroliran postopek združevanja oziroma prenosa dostopa v primeru spremembe e-poštnega naslova.

Ob deaktivaciji kontaktne osebe v MDM (npr. isActive = false) mora biti dostop do portala samodejno onemogočen. Vse spremembe statusa uporabnika morajo biti revizijsko sledljive.

Po prijavi sistem uporablja varne sejne piškotke (secure, httpOnly, sameSite) ter časovno omejitev neaktivnosti. Privzeti časovni parametri (npr. 30 minut neaktivnosti) se uskladijo z naročnikom. Sistem mora podpirati izrecno odjavo in preklic aktivnih sej.

Vsi dogodki registracije, prijave, odjave, neuspešnih poskusov prijave ter upravljanja 2FA/SSO se beležijo v varnostni dnevnik in so dostopni skrbnikom ter integrabilni v SIEM.

3.1.2.3. Ponastavitev gesla

Uporabnik lahko ponastavi pozabljeno geslo za prijavo v Portal OT s funkcionalnostjo »Pozabljeno geslo«. Postopek mora biti varen in uporabniku prijazen ter mora vključevati najmanj: (1) vnos uporabniškega imena oziroma e-poštnega naslova, (2) pošiljanje enkratne povezave ali kode z omejenim časom veljavnosti, (3) nastavitev novega gesla ob upoštevanju politik gesel, (4) obvestilo uporabniku o uspešni spremembi. Sistem ne sme razkrivati, ali uporabniški račun obstaja (enoten odziv). Poskusi ponastavitve se omejujejo (rate limiting) in

beležijo. Ponastavitev drugega faktorja (2FA) se izvaja ločeno po nadzorovanem postopku (npr. skrbniški poseg z revizijsko sledjo).

3.1.2.4. Ravni pravic in upravljanje z uporabniki

V zasebnem delu portala imajo uporabniki lahko različne privilegije/pravice dostopa. Ob kreiranju OBS in OBPS se preko vloge določi prvega uporabnika, ki ga imenujemo »privilegiran uporabnik«. Prvi uporabnik se vnese v aplikacijo preko sinhronizacije z MDM. Ta ima pravice dostopa do urejanja kontaktov ter izdajo zahtevkov za registracijo novih uporabnikov. S to pravico uporabniku omogočamo dodajanje, urejanje in pregled uporabnikov portala za svoje podjetje. To pravico ima lahko več uporabnikov v posameznem podjetju. Zahteve o spremembi ali dodajanju kontakta podane s strani uporabnika se imenujejo vloge. Oddane vloge mora administrator odobriti, da so spremembe vidne v sistemu.

Privilegiran uporabnik lahko ostalim uporabnikom svojega podjetja dodaja ali odvzema pravice. Pravice uporabnikov so zasnovane na način, da privilegiran uporabnik določa ostalim uporabnikom ali imajo ali nimajo dostop do posameznih strani znotraj portala.

3.1.3. Vloge/zahteve znotraj portala

Na portalu lahko uporabniki spremembe oz. zahteve urejajo preko Vlog. Privilegiran uporabnik ter uporabniki, ki imajo dodeljene ustrezne pravice, preko oddajo spodnje vloge:

- Vloga za vnos novega kontakta - v primeru dodajanja nove kontaktne osebe
- Vloga za spremembo kontakta - v primeru sprememb določenih podatkov kontaktne osebe
- Vloga za odstranitev kontakta - v primeru, da določena kontaktna oseba ne dela več v podjetju oz. ni več povezana relevantnim področjem dela
- Vloga za registracijo uporabnika OT Portala - za nove uporabnike
- Vloga za preklic uporabnika OT Portala - za odstranitev uporabnikov
- Uredi pravice na portalu - za urejanje dostopov/pravic uporabnikov
- Vloga za registracijo uporabnika v VR aplikaciji - za nove uporabnike VR aplikacije
- Vloga za preklic uporabnika VR aplikaciji - za odstranitev uporabnikov VR aplikacije

Znotraj portala se lahko spremlja status vlog. Oddane vloge so lahko v enem izmed spodnjih statusov:

- V obdelavi - vloga je podana administratorju, ki poda vlogi nov status.
- Sprejeta - vloga sprejeta s strani administratorja.
- Zavrnjena - vloga zavrnjena s strani administratorja

Delovni tokovi in akcije znotraj uporabniškega vmesnika, tako na strani (privilegiranega) uporabnika kot administratorskega uporabnika ostanejo vsebinsko enake kot pri trenutni zasnovi portala OT. Tudi povezave z zalednimi sistemi naročnika ostanejo enake. Dopušča se možnost, da izvajalec predlaga optimizacijo obstoječe zasnove, s katero pa se mora naročnik strinjati in jo potrditi.

3.1.3.1. Struktura Menu-ja portala OT

Ob vzpostavitvi mora menu imeti naslednjo strukturo:

- Domov (javni del portala, razen novic)
 - Novice (uporabniški del portala)
 - Podatki trga (več podstrani; povzame se jih iz trenutnega portala)
 - Arhiv podatkov in poročil
 - Dokumenti in povezave
- Vstop v bilančno shemo - novo
 - Vloga za OBS - novo
 - Vloga za OBPS - novo
 - Status vlog - novo
 - Postopek vstopa (samo admin) - novo
- Splošni podatki
 - Moj račun
 - Pregled kontaktnih oseb
 - Dokumenti
- Finance
 - Pregled finančnih kritij
 - Pregled bančnih izpiskov
 - Pregled zahtevkov in obvestil
 - Pregled računov
- Podatki in izračuni
 - Pregled bilančnih obračunov
 - Pregled pripomb na bilančni obračun
 - Pregled letnih poračunov
 - Pregled pripomb na letni poračun
- Nastavitve
 - Urejanje kontaktov in uporabnikov
 - Nastavitve obveščanja
 - Urejanj vlog (samo admin)
 - Urejanje uporabnikov (samo admin)
 - Sinhronizacije kontaktov (samo admin)
 - Urejanje dokumentov (samo admin)
 - Urejanje nastavitvev obveščanja (samo admin)
- Beleženje (samo admin)
 - Beleženje dostopa do datotek (samo admin)
 - Beleženje opomnikov (samo admin)

3.1.3.2. Novice in obvestila

Na portalu so v uporabniškem delu na voljo novice in obvestila operaterja trga. Administrator aplikacije ima preko portala možnost dodajanja, spreminjanja in brisanja novic. Novice so obogaten tekst, katerem je mogoče dodajati slike, povezave na relevantne vsebine ter povezave do datotek javnega dela.

3.1.3.3. Pregled dokumentov bilančne sheme

Uporabnik, ki ima pravico dostopa do te strani, bo imel pregled nad dokumenti, povezanimi z vstopom v BS. Dokumente ter izbrane metapodatke teh dokumentov lahko pregleduje v tabeli, lahko jih odpre ter tudi prenese na izbrano lokacijo svojega datotečnega sistema. Vrsta dokumentov, vir in ostala pravila, na podlagi katerih naj se prikažejo dokumenti v tem delu portala, se povzame iz trenutne rešitve.

3.1.3.4. Prikaz, pregled finančnih podatkov

Na portalu lahko uporabniki, ki imajo dodeljene ustrezne pravice, pregledujejo podatke ter odprejo in prenesejo dokumente povezane:

- s predloženimi finančnimi kritji (osnovnimi in gibljivimi),
- z bančnimi izpiski,
- z zahtevki in obvestili (o finančnih kritjih),
- z računi.

Vrsta dokumentov, vir in ostala pravila, na podlagi katerih naj se prikažejo podatki in dokumenti v tem delu portala, se povzame iz trenutne rešitve. Enako velja za delovne tokove in uporabniške akcije v uporabniškem vmesniku.

3.1.3.5. Podatki o bilančnih obračunih in letnih poračunih bilančnega obračuna

V trenutni različici portala so v segmentu »Podatki in izračuni« prisotne tri podstrani in z njimi povezane funkcionalnosti (pregled in nalaganje datotek), ki zaradi spremenjenih okoliščin niso več potrebni. Funkcionalnosti teh strani se v novi različici portala ne vzpostavi.

Pri ostalih štiri straneh, t.j. Pregled bilančnih obračunov, Pregled pripomb na bilančni obračun, Pregled letnih poračunov, Pregled pripomb na letni poračun, se za uporabnike, ki imajo pravico dostopa do teh strani, omogoči vse obstoječe vsebine in funkcionalnosti za pregledovanje podatkov, njihovo upravljanje ter oddajo pripomb, ki so vsebinsko in funkcionalno enake obstoječemu načinu. Upoštevati je potrebno obstoječa pravila prikazovanja podatkov o bilančnih obračuni in poračunih, t.j. da imajo OBS vpogled/pregled tudi BO poročil za BPS znotraj svojih BS, vendar le za obdobje, ko so te BPS podrejene posamezni BS. Pri možnostih za oddajo pripomb se upošteva roke, ki so povezani z objavo BO / LPBO. Enako velja za vse ostale funkcionalnosti (pripenjanje datotek, statusi in delovni tokovi za pregled pripomb, opomniki itd.).

3.1.3.6. Upravljanje s pripombami na BO

Vzpostavi se nova funkcionalnost za posredovanje prejetih pripomb avtomatsko in neposredno uporabnikom iz EDP in ZDS. V namenskem delu portala bi ti uporabniki morali podati svoj odgovor na prejete pripombe, ki bi se nato prenesle do skrbnikov ter tudi uporabnikov, ki so pripombe oddali. Vezano na ta proces se doda tudi potrebne roke, obveščanja in opomnike.

3.1.3.7. Obveščanja in naročilo na obveščanja

Registrirani uporabniki se lahko naročijo na raznovrstna obveščanje/»alarme«. Gre za e-mail obvestila, vsebino in besedila katerih lahko ureja administrator, in se prožijo ob različnih dogodkih, ki so podrobneje opisani v nadaljevanju.

Do te strani na portalu imajo dostop vsi uporabniki portala, ki pa se jim prikažejo le nastavitve za opomnike glede na dodeljene jim pravice/dostope.

Vsi uporabniki portala:

- NotificationType_News (Nove novice)

Uporabnik portala, ki ima pravico UserRigths_Priviligiran:

- NotificationType_ApplicationStatus (Stanje vlog za kontakte, VR, OT)

Uporabnik portala, ki ima pravico ali:

- UserRigths_FinanceKritja,
- UserRigths_FinanceRacuni,
- UserRigths_FinanceZahtevki,
- UserRigths_Financelzpiski

Imajo naslednje možnosti

- NotificationType_NewBankStatus (Novi bančni izpiski)
- NotificationType_GuaranteeDrop (Obvestilo o znižanju kritij)
- NotificationType_GuaranteeEndDate (Potek veljavnosti bančne garancije)
- NotificationType_InvoiceEndDate (Zapadlost računa (pred zapadlostjo))
- NotificationType_NewGuarantees (Zahtevek za dodatna kritja)
- NotificationType_NewFinanceInvoice (Novi račun ob sinhronizaciji - FinanceInvoiceSynchronization)

Uporabnik portala, ki ima pravico UserRigths_BO:

- NotificationType_NewBO (Novi bilančni obračuni)
- NotificationType_NewLPBO (Novi bilančni poračuni)

Uporabnik portala, ki ima pravico UserRigths_PripombeBO:

- NotificationType_ReclamationBO (Izdaja pripombe na BO)
- NotificationType_ReclamationRespBO (Odgovor na pripombo za BO)
- NotificationType_ReclamapinLPBO (Izdaja pripombe na LPBO)
- NotificationType_ReclamationRespLPBO (Odgovor na pripombo za LPBO)
- NotificationType_DueDatesBO_LPBO (Sprememba rokov za pripombe na BO in LPBO)

Uporabnik portala, ki ima pravico UserRigths_IBISAdmin

- NotificationType_PartnerSync
- NotificationType_ContactSync
- NotificationType_NewApplication (Nova vloga)

Pri naslednjih vrstah obveščanj lahko uporabnik spremeni tudi čas obveščanja:

- NotificationType_GuaranteeEndDate

- NotificationType_InvoiceEndDate
- NotificationType_NewGuarantees
- NotificationType_BSEExpiration

Pri tem so naslednje možnosti nastavitve intervala:

- Vsak delovnik
- Vsak ponedeljek
- Vsak torek
- Vsako sredo
- Vsak četrtek
- Vsak petek
- Samo enkrat

Pri ostalih vrstah obveščanja se pošiljanje e-pošte dogodi takoj, ko se dogodek sproži.

V novi rešitvi se ohrani tudi ostale funkcionalnosti, delovne tokove, vmesnik, nastavitve in pravila, ki so vezane na opomnike. Potrebno je prevzeti način določitve začetnega nabora predizbranih opomnikov, ko se ustvari nov uporabnik, zagotoviti možnost odjave na posamezni opomnik preko povezave, ki bo vsebovana v e-mailu opomnika, zagotoviti, da se opomnik pošlje tudi v primeru, da ni poštni strežnik v danem trenutku ne deluje (zamik pošiljanja) itd.

3.1.4. Administratorski (skrbniški) del portala

S prenovo se smiselno ohrani funkcionalnosti, ki jih glede administracije in konfiguracije nastavitev podpira DNN. V upravljaljskem delu portala je omogočeno:

- Urejanje menija,
- Urejanje vsebine in novic (z možnostjo uporabe obogatenejšega teksta, kateremu je mogoče dodajati slike, povezave na relevantne vsebine ter povezave do datotek javnega dela),
- Urejanje javnega in privatnega dela dostopa,
- Urejanje dizajna in grafičnih tem,
- Namestitve modulov,
- Dodajanje novih spletnih mest (npr. pri dodajanju novega jezika),
- Sistemske nastavitve portala in drugo.

3.1.4.1. Dodajanje, registracija in prijava administratorja

Delovni tok za dodajanje, registracijo in prijavo administratorskega uporabnika se izvede preko IBIS++ aplikacije. Uporabnik v IBIS++ aplikaciji ima s svojim uporabnikom avtomatski dostop tudi do administratorskih strani portala OT.

Vzpostavi se dve ravni administratorjev oz. skrbnikom. Privilegirani administrator/skrbnik ter (navadni) administrator/skrbnik. Privilegirani administratorji imajo v portalu OT in aplikaciji pravice in dostop do vseh (administratorskih) strani portala in aplikacije, medtem ko ima (navadni) administratorji le pravice in dostope, ki jim jih dodeli privilegirani uporabnik (ta raven pravic je namenjena sodelavcem iz drugih oddelkov/služb, ki ne potrebujejo vpogleda v vse podatke).

Administratorjem se lahko znotraj aplikacije dodeli tudi »SuperUser« atribut. V tem primeru ima uporabnik na portalu možnost urejanje strani (dodajanje strani, menujev, CMS vsebine, spreminjanje modulov, konfiguracije portala itd.).

3.1.4.2. Urejanje vlog

Administrator lahko pregleduje vloge v tabeli vlog. V tabeli so oz. bodo navedeni naslednji tipi vlog:

- Vloga za registracijo OBS
- Vloga za registracijo OBPS
- Vloga za vnos kontakta
- Vloga za spremembo kontakta
- Vloga za odstranitev kontakta
- Vloga za registracijo uporabnika VR aplikacije
- Vloga za preklic uporabnika VR aplikacije
- Vloga za registracijo uporabnika portala OT
- Vloga za preklic uporabnika portala OT

Vsaka vloga ima svojo šifro vloge (črtno kodo oziroma serijsko številko), partnerja (ki je kreiral vlogo), datum izdelave vloge ter status vloge. Določene vloge imajo dokument PDF, določene pa ne.

Vse vloge pregleda admin ter te odobri ali zavrne. V kolikor proces preverjanja vloge traja dalj časa, lahko admin vlogi spremeni status v »v obdelavi«. Vloge imajo lahko tako naslednje statuse (dbo.CodeList):

- StateType_Oddana (oddana)
- StateType_VObdelavi (v obdelavi)
- StateType_Sprejeta (sprejeta)
- StateType_Zavrnjena (zavrnjena)

Pravila prehod med različnimi statusi vlog se prevzamejo iz obstoječe rešitve.

Pri vsaki izdelavi vloge lahko uporabnik doda komentar k vlogi. Enako lahko za vsako spremembo stanja vloge tudi admin doda komentar, ki bo nato viden tudi uporabniku.

Vmesnik za pregledovanje in urejanje vlog so različni glede na vrsto vloge. Trenutne vmesnike se ohrani tudi v novi rešitvi, z razliko za vloge za OBS in OBPS, pri katerih se vmesnike in delovne tokove določi in izvede v okviru tega projekta.

Enako se ohranijo tudi vsi delovni tokovi in akcije na uporabniškem vmesniku. Ohrani se tudi pravila (pravila za generiranje serijskih številke - šifre, črtne kode,...), vsebine in prikazi v tabelah ter ostali elementi vmesnika.

3.1.4.3. Urejanje in sinhronizacija kontaktov (kontaktnih oseb)

Admin/skrbnik lahko pregleda kateri kontakti so sinhronizirani na portalu (oziroma IBIS rešitev) ter ureja pravice dostopa. Vse ostale kontaktne informacije se urejajo znotraj MDM, ali preko sistema vlog (integracija s portalom OT), ali preko ročnega vnosa v MDM.

Pravila in način sinhronizacije med podatki portala ter MDM ostanejo taki, kot so v trenutni rešitvi. Vsem tem vlogam je skupno, da je MDM ID kontakta že znan in je tako pri sinhronizaciji med MDM in IBIS točno določen za kateri kontakt se spreminjajo atributi. Denimo:

- Vloga za spremembo kontakta vpliva na attribute, kot so Ime, Priimek, e-pošta, telefon, GSM, vloge (»role«) kontaktne osebe
- Vloga za odstranitev kontakta vpliva na atribut isActive
- Vloga za registracijo uporabnika VR aplikacije vpliva na atribut isVRUser
- Vloga za preklic uporabnika VR aplikacije vpliva na atribut isVRUser
- Vloga za registracijo uporabnika portala OT vpliva na atribut isPortalUser
- Vloga za preklic uporabnika portala OT vpliva na atribut isPortalUser

Sinhronizacija kontaktov vedno poteka iz MDM proti portalu. Medtem ko iz portala proti MDM poteka prenos podatkov preko vlog.

Sinhronizacije kontaktov iz MDM se proži ob izbranem terminu in periodi, ali pa na zahtevo. Pri proženju sinhronizacije z MDM vsi kontakti v MDM bazi, ki so bili posodobljeni glede na zadnji datum MDM sinhronizacije prenesejo v vmesni tabelo na portalu. Skrbnik lahko sproži sinhronizacijo s klikom na gumb »Sinhroniziraj MDM«. Iz vmesnika so razvidni kontakti, pri katerih je prišlo do spremembe. Skrbnik nato lahko izbere tiste kontakte, pri katerih želi spremembo sinhronizirati na portal oziroma spremembo zavrne.

3.1.4.4. Urejanje dokumentov

Skrbnik ima možnost pregleda vseh dokumentov, ki se objavijo v uporabniškem delu portala. Vsi ti dokumenti se po vnaprej določeni poti sinhronizirajo s portalom oziroma aplikacijo IBIS++. Vrste dokumentov, ki se sinhronizirajo, pravil in način sinhronizacije se uredijo na enak način kot je to urejeno v obstoječi rešitvi.

3.1.4.5. Nastavitve opomnikov in obvestil

Skrbnik ima na namenski strani vmesnika možnost urejanja nastavitve opomnikov in obvestil, torej čas izvršitve ter vsebino sporočila. Na voljo morajo ostati vsi opomniki iz trenutne rešitve, vključno z možnostmi nastavitvev (vrsta opomnika, čas pošiljanja, perioda pošiljanja, naslovnik/uporabnik, ki prejme tak opomnik itd.). Dodana mora biti možnost, da skrbnik označi, če je posamezni opomnik dodeljen kot prednastavljeno izbran ob ustvarjanju novega uporabnika oz. mora biti dodana matrika, v kateri bo lahko skrbnik lahko določil kateri opomniki so prednastavljeni ob dodelitvi določenih pravic uporabnikom.

Pri določenih opomniki si uporabnik ne more sam spreminjati nastavitve pošiljanja, ker so vezani na določen dogodek (nova vloga, nov BO itd.)

Skrbnik ima možnost pregleda poslanih sporočil/opomnikov in sporočil v pošiljanju.

Ob izdelavi sporočila oziroma opomnika, se e-pošta vedno vnese v čakalno vrsto. Na ta način je zagotovljeno, da je na voljo seznam vseh poslanih sporočil, hkrati pa se zagotovi, da se v primeru izpada servisa za pošiljanje pošte, to pošto pošlje ob naslednjem ciklu pošiljanja.

Skrbnik ima na voljo vmesnik, v katerem lahko besedilo vsakega obvestila uredi. Urejeni so tudi »ključki«, ki jih lahko uporabi, da se v obvestilu prikažejo določeni podatki, vezani na uporabnika, BO, določen postopek itd. Omogočena je večjezičnost.

3.1.4.6. Beleženje dostopa do datotek

Skrbnik ima možnost pregleda zgodovine dostopa do datotek uporabnikov znotraj uporabniškega dela portala, administratorskega dela portala ter IBIS aplikacije.

3.2. Funkcionalne zahteve (FR) za aplikacijo za bilančni obračun IBIS++

ID	Zahteva	Prioriteta	Povzetek	Preverjanje
FR-APP-001	Struktura menu-ja	OBVEZNO	Ohraniti je treba strukturo menijev in modulov aplikacije, prilagojeno novi platformi.	Pregled + SAT
FR-APP-002	Jedrne funkcionalnosti	OBVEZNO	Aplikacija mora ohraniti jedrne funkcionalnosti: uvozi, validacije, izračuni BO/LPBO, poročila in nastavitve.	SAT
FR-APP-003	Podprte funkcije/izračuni	OBVEZNO	Zagotovi se enaka podpora izračunov in poslovnih pravil kot v obstoječi rešitvi (brez spremembe rezultatov).	Regresijski test
FR-APP-004	Kontrole izračunov	OBVEZNO	Vzpostaviti je treba kontrole izračunov in poročila za dokazovanje	Regresijski test + SAT

			pravilnosti (kontrola sistema).	
FR-APP-005	Upravljanje uporabnikov aplikacije - skrbnikov	OBVEZNO	Skrbniško upravljanje uporabnikov in vlog aplikacije, povezava na IAM/SSO, ter revizijska sled sprememb pravic.	Varnostni test + pregled
FR-APP-006	Partnerji	OBVEZNO	Modul partnerjev mora podpirati pregled in urejanje podatkov v skladu s pravili ter integracijo z MDM.	Integracijski test
FR-APP-007	Bilančna shema	OBVEZNO	Vzpostavi se modul za upravljanje BS/BPS in povezanih pravil, skladno z obstoječo aplikacijo.	Funkcionalni test
FR-APP-008	Prezemno-predajna mesta	OBVEZNO	Vzpostavi se upravljanje PPM, deležev dobave in vseh povezanih pravil/validacij.	Funkcionalni test
FR-APP-009	Proces bilančnega obračuna	OBVEZNO	Celoten proces BO (uvozi, nastavitve, izračun, poročila, objave, pripombe) se ohrani in je izveden na novi platformi.	SAT
FR-APP-010	Proces letnega poročuna bilančnega obračuna (LPBO)	OBVEZNO	Celoten proces LPBO se ohrani in je izveden na novi platformi z enakimi rezultati in poročili.	SAT

FR-APP-011	Uvozi podatkov in datotek	OBVEZNO	Podprti so vsi obstoječi uvozi (datoteke/API), validacije, obdelava napak in ponovitev uvozov.	Integracijski test
FR-APP-012	Modul EIP (elektronska izmenjava podatkov)	OBVEZNO	Vzpostavi se modul EIP za elektronsko izmenjavo podatkov in objavo poročil prek dogovorjenih vmesnikov.	Integracijski test
FR-APP-013	Dnevnik uvozov	OBVEZNO	Na voljo je dnevnik uvozov z možnostjo filtriranja, vpogleda v napake in ponovitev.	Funkcionalni test
FR-APP-014	Nastavitve	OBVEZNO	Upravljanje nastavitvev (sinhronizacije, roki, prevodi, obračunski interval) se ohrani in omogoča revizijsko sled sprememb.	Pregled + test

Aplikacija za bilančni obračun IBIS++ je namenjena:

- prejemu, validaciji in uvozu podatkov od elektrooperaterjev,
- izračun bilančnega obračuna (nastavitve, izračuni),
- izračun letnega poročuna bilančnega obračuna,
- priprava rezultatov BO in LPBO za člane trga (poročila, podatki),
- urejanje sistemskih nastavitvev

3.2.1. Struktura menu-ja

Osnovni menu mora v novi rešitvi ohraniti naslednjo strukturo:

- Bilančna shema, Partnerji, Pogodbe, Primopredajna mesta
- Bilančni obračun (Obdobja, Izračun)
- Letni poročun bilančnih obračunov
- Uvozi podatkov

- Nastavitve
- Uporabniki

3.2.2. Jedrne funkcionalnosti

Osnovne funkcionalnosti, ki se izvajajo na aplikacijskem strežniku so metode, vezane na izračun BO in LPBO. Enako kot na portalu morajo tudi v aplikaciji vse tabele, ki bodo prikazane, omogočiti razvrščanje in (smiselno) filtriranje glede na vse parametre v stolpcih. Omogočeni morajo biti tudi izvozi v razširjene formate (xlsx, csv, xml ipd.).

3.2.3. Podprte funkcije/izračuni

Trenutni izračuni in funkcije, ki jih omogoča in podpira zdajšnja rešitev, morajo biti prenesene tudi v novo rešitev. Slednje mora zajemati najmanj:

- izračun osnovnih cen odstopanj,
- izračun odjema, oddaje in realizacije,
- izračun tržnega plana in korigiranega tržnega plana
- izračun odstopanj
- izračun zneskov bilančnega obračuna
- izračun kontrol.

Vsi izračuni izhajajo iz veljavnih Pravil za delovanje trga z električno energijo in morajo biti ustrezno preneseni v novo rešitev. Funkcije, opisane v naslednjih poglavjih, sprejmejo vhodne podatke v obliki seznamov, in vrnejo specificirane rezultate v primerni podatkovni obliki. Servisi ob zagonu poskrbijo za črpanje, pripravo in agregacijo ustreznih podatkov iz podatkovnih virov glede na izbrano obdobje, bilančno skupino ipd. Na tako pripravljenih podatkih uporabijo ustrezne funkcije, ki napravijo zahtevane izračune.

Podpreti je potrebno tudi izračune in priprave poročil, ki jih aplikacija izvede ob izvedbi bilančnih izračunov, t.j. poročila za FRS, ELES, AGEN, povzetek BO ter vsa poročila, vezana na člane bilančne sheme, kot so BO poročilo za BS, za BPS, priloge k računom BS.

Obravnava prehoda med zimskim/letnim časom, upoštevanje pravilne dolžine obračunskega intervala in pravilne dolžine obračunskega obdobja spadajo med pripravo podatkov in se jo izvede v servisu pred klicem funkcije.

Iz trenutne rešitve se v novo rešitev prenese naslednje metoda izračuna cen odstopanj:

- Enojna cena po pravilih 2022
- Dvojna cena po pravilih 2022 izravnavava v obe smeri
- Dvojna cena po pravilih 2022 finančna nevtrálnost
- Enojna cena 2025 - izravnavave s platformami

Iz obstoječe rešitve se prevzame vse nastavitve, validacije in pravila izračunov.

Doda se še metoda »Dvojna cena 2025 - izravnavave v obe smeri s platformami« ter »Dvojna cena 2025 - izravnavave s platformami - finančna nevtrálnost«. Pri teh dveh metodah se enako

kot gre pri metodah po dvojnih cena po pravilih 2022 samo upošteva možnost uvoza cen odstopanj, izračunanih izven aplikacije, ob upoštevanju cen izravnave s platform. V okviru projekta se določi morebitne dodatne validacije.

3.2.4. Kontrole izračunov

Vsa preverjanja vhodnih podatkov za izračune ter pravilnost izračunov se v novi rešitvi vzpostavijo metode oz. kontrole iz obstoječe aplikacije. To obsega najmanj naslednje kontrole:

- Kontrola sistema
- Kontrola odstopanj
- Kontrola omrežji
- Kontrola realizacij
- Kontrola ELES
- Kontrola ND (neregulirane dobave)
- Kontrola ND PPM
- Kontrola izravnave
- Kontrola tržnega plana

3.2.5. Upravljanje uporabnikov aplikacije - skrbnikov

V aplikaciji je ena raven pravic, in sicer je uporabnik hkrati tudi administrator (skrbnik). Skrbnik ima tako na voljo vse funkcionalnosti aplikacije. Skrbnik je hkrati administrator portala OT.

Uporabnik/skrbnik ima na voljo pogled na seznam vseh uporabnikov/skrbnikov aplikacije. Skrbnik lahko dodaja nove uporabnika v sistem. Uporabniku (novemu skrbniku) nastavi predvidene attribute.

3.2.6. Partnerji

Skrbniki lahko pregledujejo, urejajo ter dodajajo partnerje. Partnerja je v aplikacijo mogoče dodati preko sinhronizacije z MDM bazo podatkov, kjer so ti partnerji že vneseni. Način in pravila sinhronizacije iz MDM se povzamejo/prenesejo iz trenutne rešitve.

Skrbnik lahko tudi ročno doda partnerja ter ureja attribute parametrov partnerja. Uporabnik lahko ureja vsa polja razen IDja partnerja ter datuma vnosa in datuma zadnje spremembe.

3.2.7. Bilančna shema

Skrbniki imajo pregled nad bilančno shemo ter pogodbami med partnerji bilančne sheme. Skrbnik pogodbo o članstvu v bilančni shemi doda in ureja v aplikaciji. Bilančna shema v aplikaciji je lahko različna od tiste na portalu in je specifično vezana na izdelavo BO. Na portal se bilančna shema prenaša iz MDM baze.

3.2.8. Primopredajna mesta

Prevzemno predajana mesta (PPM) so tisti elementi v bazi, na katere se uvaža časovne vrste podatkov. Iz obstoječe rešitve se smiselno prenese in vzpostavi vse funkcionalnosti ter pravila iz trenutne rešitve. Prenesejo se tudi vsi šifranti povezani s PPM. Skrbniki imajo v aplikaciji

možnost vnosa, pregleda, urejanja in ostalega upravljanja s primopredajnimi mesti (PPM). Skrbniki lahko urejajo vse attribute PPMja, razen PPM IDja.

PPMji imajo lahko različne deleže dobave. Skrbniki lahko urejajo te deleže, pomembno je le, da skupni delež vseh dobaviteljev enak 100%, kar se validira preden se deleži shranijo. Urejeno mora biti tudi verzioniranje. Za vsako spremembo PPMja oziroma vrstice PPMja, se sprememba zapiše tudi v arhivsko tabelo za spremljanje sprememb. Spremembe se spremljajo na nivoju teksta (obveščanje o spremembah) in ne na nivoju šifriranja IDjev (ponovitve izračunov glede na preteklo stanje).

3.2.9. Proces bilančnega obračuna

Zaokroževanje podatkov - vsa pravila vezana na zaokroževane podatkov pri procesih uvoza, priprave podatke, pri izračunih ter ostalih postopkih morajo ostati identični kot v trenutni rešitvi.

Poimenovanje datotek - iz obstoječe rešitve se prenesejo tudi vsa pravila vezana na poimenovanja datotek.

Obdobja bilančnega obračuna - rešitev mora omogočati vse funkcionalnost vezane na ustvarjanje in upravljanje obračunskih obdobji, vključno z vmesnikom, na enak način kot obstoječa rešitev. Enako velja za vsa pravila, ki so povezana s tem elementom (validacije, možnosti urejanja, brisanja itd.).

Vmesnik za bilančni obračun - nova rešitev mora omogočiti in podpreti vnos in upravljanje enakih parametrov za bilančni obračun kot obstoječa aplikacija. Zagotoviti je potrebno tudi vse validacije in s tem povezana pravila in obvestila in ostalih vizualni elementi (semaforji, opozorilna okna) iz trenutne rešitve. Vmesnik se v okviru projekta v dogovoru z naročnikom prilagodi glede na zadnje stanje procesa bilančnega obračun (denimo, odstrani se določene neaktualne check-box kot »izračun korekcije cen«).

Postopek izračuna - po sprožitvi izračuna BO se iz obstoječe rešitve prenesejo vsi koraki postopka (validacije, obveščanja, logiranje). Hitrost izračuna ne sme biti daljša od performance trenutne rešitve.

V novi rešitvi se proces razdeli v dva koraka, izračun BO ter pripadajoča poročila ter pripravo poročil za partnerje.

Izdelava poročil - nabor, formate, postopek in način ustvarjanja poročil iz obstoječe aplikacije mora, razen kjer je to drugače zahtevano, biti vzpostavljen na enak način tudi v novi rešitvi. Vsa poročila izdeluje aplikacija sama, brez uporabe in navezave na druge, zunanje rešitve (npr. Strategy).

Poročila za člane - Rešitev mora omogočati pri posameznem poročilu, ki se nanaša na člana sheme, uporabo predlog v različnih jezikih. Izbor predloge je pri posameznem partnerju odvisen od jezika, ki je izbran/določen pri posameznem partnerju znotraj aplikacije. Predloge iz trenutne aplikacije se uporabi tudi v novi rešitvi, to pomeni, da se v vsaki datoteki so ob

osnovnem listu, kjer so osnovni podatki o BO, tudi listi, kjer so pripravljeni podatki realizacije po distribucijskih območjih ter zavihek z realizacijo na prenosnem območju. Po enakem načelu kot v trenutni rešitvi, mora veljati, da v primeru, da posamezna BS ali BPS nima katerih od predvidenih skupin podatkov, so ta polja prazna, skrita ali slabše vidna (namesto črne barve se uporabi npr. siva). V primeru da BS ali BPS nima realizacije na distribucijskih območjih ali prenosnem omrežju, lista, kjer so predvideni ti podatki, ni zraven.

Digitalno potrjevanje poročil za člane - poročila za člane, ki se odloži oz. so po potrditvi dostopni uporabnikom članov BS na portalu OT, morajo biti digitalno podpisani oz. potrjeni. Trenutni način potrjevanje preko digitalne potrdila se nadomesti z ustrezno, ekvivalentno rešitvijo digitalnega potrjevanja.

Dokumenti/poročila za finančno poravnavo - v novi rešitvi se vzpostavijo enaka pravila, postopki, predloge in nastavitve, kot v obstoječi aplikaciji.

Poročilo Kontrole sistema - ob vsakem izračunu BO se izvede in ustvari tudi datoteko, v kateri so prikazana vse predvidene kontrole izračunov ter primerjave in pregledi vhodni podatkov. Nova rešitev mora vzpostaviti enako ali v dogovoru z naročnikom v določenih delih prilagojeno predlogo tega poročila. Predloga tega dokumenta mora biti povezana z metodo izračuna. Vsaka metoda izračuna BO ima (lahko) svojo predlogo dokumenta kontrol.

Poročilo povzetek BO - ob vsakem izračunu BO se izvede in ustvari tudi datoteko, v kateri so prikazani ključni podatki BO. Nova rešitev mora vzpostaviti enako ali v dogovoru z naročnikom v določenih delih prilagojeno predlogo tega poročila. Predloga tega dokumenta mora biti povezana z metodo izračuna. Vsaka metoda izračuna BO ima (lahko) svojo predlogo povzetka BO.

Poročilo za Agencijo - ob vsakem izračunu BO se izvede in ustvari tudi datoteko, ki je namenjena poročanju podatkov BO na Agencijo. Pri tem poročilu se v okviru projekta dogovori prilagoditve glede na dodatne PPM, ki niso še vključeni v poročilu. Hkrati se bo z Agencijo dogovoril tudi prehod iz formata iz xlsx na xml.

Objave podatkov na EIP - funkcionalnosti iz obstoječe aplikacije vezane na modul »elektronske izmenjave podatkov« se na enak način vzpostavi tudi v novi rešitvi.

Umik/preklic objave BO - vse obstoječe funkcionalnosti vezane na postopek preklica objavljenega BO, vključno z obveščanji članov preko portala in opomnikov, se vzpostavijo tudi v novi rešitvi.

Obravnava pripomb na BO - vse obstoječe funkcionalnosti vezane na postopek oddaje, obravnave, upravljanja s pripombami, nastavitvami (rokov in ostalo), obveščanji in prikazih na portalu, se vzpostavijo tudi v novi rešitvi ob upoštevanju predhodno omenjenega načina nadgradnje tega procesa.

Poročilo ELES in poročilo za FRS - ob vsakem izračunu BO se izvede in ustvari tudi omenjeni poročili, skladno s posamezno predlogo in dogovorjeno vsebino. Nova rešitev mora vzpostaviti enako ali v dogovoru z naročnikom v določenih delih prilagojeno predlogo tega poročila.

Predloga tega dokumenta mora biti povezana z metodo izračuna. Vsaka metoda izračuna BO ima (lahko) svojo predlogo povzetka BO.

Prenos podatkov v DWb - v novi rešitvi se vzpostavi možnost »push-a« podatkov o BO na enak način kot v trenutni rešitvi. V okviru projekta se dogovori o morebitni prilagoditvi nabora podatkov (dodatni PPM), ki se jih pripravi za prenos v DWb.

Primerjave BO - v novi rešitvi se vzpostavi funkcionalnost za primerjave serij dveh izbranih BO. V novi rešitvi se določi in vzpostavi aktualen nabor serij. Končni nabor se določi v okviru projekta. Ob tem se razširi možnost nabora po vrsti PPM, na način da bo možno primerjati tudi PPM, ki so vezani na meritve, izravnavo itd.

3.2.10. Proces letnega poročila bilančnega obračuna (LPBO)

Zaokroževanje podatkov - vsa pravila vezana na zaokroževanje podatkov pri procesih uvoza, priprave podatke, pri izračunih ter ostalih postopkih morajo ostati identični kot v trenutni rešitvi.

Poimenovanje datotek - iz obstoječe rešitve se prenesejo tudi vsa pravila vezana na poimenovanja datotek.

Obdobja LPBO - rešitev mora omogočati vse funkcionalnost vezane na ustvarjanje in upravljanje obračunskih obdobji, vključno z vmesnikom, na enak način kot obstoječa rešitev. Enako velja za vsa pravila, ki so povezana s tem elementom (validacije, možnosti urejanja, brisanja itd.).

Vmesnik za LPBO - nova rešitev mora omogočiti in podpreti vnos in upravljanje enakih parametrov za LPBO kot obstoječa aplikacija. Zagotoviti je potrebno tudi vse validacije in s tem povezana pravila in obvestila in ostalih vizualni elementi (semaforji, opozorilna okna) iz trenutne rešitve. Vmesnik se v okviru projekta v dogovoru z naročnikom prilagodi glede na zadnje stanje procesa LPBO.

Postopek izračuna - po sprožitvi izračuna LPBO se iz obstoječe rešitve prenesejo vsi koraki postopka (validacije, obveščanja, logiranje). Hitrost izračuna ne sme biti daljša od performance trenutne rešitve.

V novi rešitvi se proces razdeli v dva koraka, izračun LPBO ter pripadajoča poročila ter pripravo poročil za partnerje.

Izdelava poročil - nabor, formate, postopek in način ustvarjanja poročil iz obstoječe aplikacije mora, razen kjer je to drugače zahtevano, biti vzpostavljen na enak način tudi v novi rešitvi. Vsa poročila izdeluje aplikacija sama, brez uporabe in navezave na druge, zunanje rešitve (npr. Strategy).

Poročila za člane - Rešitev mora omogočati pri posameznem poročilu, ki se nanaša na člana sheme, uporabo predlog v različnih jezikih. Izbor predloge je pri posameznem partnerju odvisen od jezika, ki je izbran/določen pri posameznem partnerju znotraj aplikacije. Predloge iz trenutne aplikacije se uporabi tudi v novi rešitvi. Po enakem načelu kot v trenutni rešitvi,

mora veljati, da v primeru, da posamezna BS ali BPS nima katerih od predvidenih skupin podatkov, so ta polja prazna, skrita ali slabše vidna (namesto črne barve se uporabi npr. siva). V primeru da BS ali BPS nima realizacije na distribucijskih območjih ali prenosnem omrežju ali niso dobavitelji za izgube, teh podatkov ni na poročilu.

Digitalno potrjevanje poročil za člane - poročila za člane, ki se odloži oz. so po potrditvi dostopni uporabnikom članov BS na portalu OT, morajo biti digitalno podpisani oz. potrjeni. Trenutni način potrjevanje preko digitalne potrdila se nadomesti z ustrezno, ekvivalentno rešitvijo digitalnega potrjevanja.

Dokumenti/poročila za finančno poravnavo - v novi rešitvi se vzpostavi pravilo, da se ti dokumenti ustvarijo le v primeru, da je izdelan LPBO s statusom LPBO2 (t.j. končni LPBO; pri LPBO je drugačna logika kot pri BO; finančna poravnava nastopi pri končnem LPBO (LPBO2), pri prvem, informativnem LPBO (LPBO1), pa ni finančne poravnave). Temu ustrezno se prilagodijo vse objave, obveščanja, opomniki, na portalu.

Kontrolna poročila - ob vsakem izračunu LPBO se izvedejo in ustvarijo tudi datoteke, v katerih so prikazane vse predvidene kontrole izračunov ter primerjave in pregledi vhodni podatkov. Nova rešitev mora vzpostaviti enake ali v dogovoru z naročnikom v določenih delih prilagojene predloge tega poročila.

Poročilo povzetek LPBO - ob vsakem izračunu LPBO se izvede in ustvari tudi datoteka, v kateri so prikazani ključni podatki LPBO. Nova rešitev mora vzpostaviti enako ali v dogovoru z naročnikom v določenih delih prilagojeno predlogo tega poročila.

Objave podatkov na EIP - funkcionalnosti iz obstoječe aplikacije vezane na modul »elektronske izmenjave podatkov« se na enak način vzpostavi tudi v novi rešitvi.

Umik/preklic objave LPBO - vse obstoječe funkcionalnosti vezane na postopek preklica objavljenega LPBO, vključno z obveščanji članov preko portala in opomnikov, se vzpostavijo tudi v novi rešitvi.

Obravnava pripomb na LPBO - vse obstoječe funkcionalnosti vezane na postopek oddaje, obravnave, upravljanja s pripombami, nastavitvami (rokov in ostalo), obveščanji in prikazih na portalu, se vzpostavijo tudi v novi rešitvi ob upoštevanju predhodno omenjenega načina nadgradnje tega procesa.

3.2.11. Uvozi podatkov in datotek

Aplikacija za BO operira z več različnimi vhodnimi podatki, ki jih je potrebno pravočasno prejeti, ustrezno preveriti in validirati, obdelati in uvoziti v podatkovno bazo aplikacije. Viri podatkov so različni, priskrbijo jih različni deležniki. V nadaljevanju so navedeni posamezni sklopi vhodnih podatkov ter pričakovane funkcionalnosti nove rešitve v povezavi s procesom prejema in obdelave le-teh.

Meritve distribucijskih območji (EDP in ZDS) - vzpostavi se funkcionalnosti za uvoze podatkov iz dist. območji na enak način kot v obstoječi rešitvi. Znotraj aplikacije se izdelajo xlsx predloge

prilagojene za vsako distr. obm. posebej. Vsaka ima določen nabor PPM glede na prisotnost dobaviteljev (članov BS) na posameznem območju ter ob upoštevanju vseh povezav (ND) do ostalih omrežji. Vmesnik, postopek uvoza, validacije, pravila in ostale nastavitve iz obstoječe aplikacije se smiselno vzpostavijo tudi v novi rešitvi. Uvozi podatkov so mogoči preko xlsx ter EIP (t.j. modula za elektronsko izmenjavo podatkov). Za primere uvoza preko EIP se pripravi tudi možnost izvoza teh podatkov v predlogi, ki je po strukturi identična uvozni predlogi.

Podatki iz distribucijskih območji (EDP in ZDS) za potrebe LPBO - vzpostavi se funkcionalnosti za uvoze podatkov iz dist. območji na enak način kot v obstoječi rešitvi. Znotraj aplikacije se izdelajo xlsx predloge prilagojene za vsako distr. obm. posebej. Vsaka ima določen nabor PPM glede na prisotnost dobaviteljev (članov BS) na posameznem območju ter ob upoštevanju vseh povezav (ND) do ostalih omrežji. Vmesnik, postopek uvoza, validacije, pravila in ostale nastavitve iz obstoječe aplikacije se smiselno vzpostavijo tudi v novi rešitvi. Uvozi podatkov so mogoči preko xlsx ter EIP (t.j. modula za elektronsko izmenjavo podatkov). Za primere uvoza preko EIP se pripravi tudi možnost izvoza teh podatkov v predlogi, ki je po strukturi identična uvozni predlogi.

Podatki (meritve) na prenosnem omrežju (ELES) - vzpostavi se funkcionalnosti za uvoze podatkov iz prenosnega omrežja na enak način kot v obstoječi rešitvi. Znotraj aplikacije se izdelajo xlsx predloga, ki vsebuje vse izbrane PPM. Vmesnik, postopek uvoza, validacije, pravila in ostale nastavitve iz obstoječe aplikacije se smiselno vzpostavijo tudi v novi rešitvi. Uvozi podatkov so mogoči preko xlsx.

Podatki o tržnih planih (Borzen, VR app ali DWWh) - vzpostavi se funkcionalnosti za uvoze podatkov o tržnih planih na enak način kot v obstoječi rešitvi. Znotraj aplikacije se izdelajo xlsx predloga, ki vsebuje vse izbrane PPM. Vmesnik, postopek uvoza, validacije, pravila in ostale nastavitve iz obstoječe aplikacije se smiselno vzpostavijo tudi v novi rešitvi. Uvozi podatkov so mogoči preko xlsx. Uvoz podatkov je omogočen tudi preko integracije z DWWh. Za primer uvozov iz DWWh se vzpostavi poročilo, ki se ga bo lahko izvozilo in v katerem bodo zbrani uvoženi podatki iz DWWh.

Podatki o izravnavi in regulaciji (ELES) - vzpostavi se funkcionalnosti za uvoze podatkov iz prenosnega omrežja na enak način kot v obstoječi rešitvi. Znotraj aplikacije se izdelajo xlsx predloga, ki vsebuje vse izbrane PPM. Vmesnik, postopek uvoza, validacije, pravila in ostale nastavitve iz obstoječe aplikacije se smiselno vzpostavijo tudi v novi rešitvi. Uvozi podatkov so mogoči preko xlsx.

Uvoz SIPX (vir BSP Southpool) - vzpostavi se novo funkcionalnosti za uvoz podatkov o SIPX. Dogovori se nov način črpanja podatkov (preko API) ali novo predlogo za podatke, iz katere bo aplikacija prebrala in uvozila SIPX. Podrobnosti funkcionalnosti izvajalec in naročnik določita v okviru projekta.

Cene odstopanj (Borzen) - vzpostavi se funkcionalnosti za uvoze podatkov o cenah odstopanj, za primere izračunov cen odstopanj skladno s Pravili za delovanje trga, ki pa niso podprti v aplikaciji, in sicer na enak način kot v obstoječi rešitvi. Znotraj aplikacije se izdelajo xlsx predloga,

ki vsebuje vse PPM za cene odstopanj. Vmesnik, postopek uvoza, validacije, pravila in ostale nastavitve iz obstoječe aplikacije se smiselno vzpostavijo tudi v novi rešitvi.

V trenutni aplikaciji sta prisotna še dva sklopa vhodnih podatkov, za katere v novi aplikaciji ni potrebno zagotoviti uvozov, in sicer za podatke o izpadih ter koeficiente izgub.

3.2.12. Modul EIP (elektronska izmenjava podatkov)

V novi rešitvi se vzpostavi modul EIP z enakimi funkcionalnostmi kot jih ima v obstoječi rešitvi. Vzpostavi se delujoč spletni servis do rešitve CEEPS, ki ga upravlja Informatika. Zagotovi se, da so podprti vsi standardi in postopki izmenjave, ki že delujejo v okviru trenutne rešitve. Vzpostavi se tudi spletni servis oz. izmenjavo podatkov z Agencijo, in sicer za mesečno posredovanje podatkov o BO. Zagotovi se uporabniku prijazen vmesnik, ki bo omogočal pregledno in učinkovito pregledovanje in iskanje izmenjenih podatkov ter tudi pregled in možnost upravljanja z nastavitvami spletnih servisov.

3.2.13. Dnevnik uvozov

V novi rešitvi se vzpostavi t.i. dnevnik uvozov, to je pregledovalnik vseh sklopov podatkov, ki so bili uvoženi v bazo aplikacije kot vhodni podatki, tako za BO kot LPBO. Vzpostavi se vse funkcionalnosti, pravila, preglede kot v obstoječi rešitvi.

3.2.14. Nastavitve

V novi rešitvi se vzpostavi celoten nabor nastavitvev, kot izhaja iz nadaljevanja. Pri vseh je osnova trenutna rešitev aplikacije.

Konfiguracija sinhronizacij - aplikacija se mora povezovati, črpati in zapisovati (v nadaljevanju bo za zapisano uporabljen krovni pojem sinhronizacija) podatke v različne zaledne sisteme. V namenskem vmesniku se priprave pregled vseh integracij z ostalimi sistemi, pri vsakem mora biti dodana možnost določitve nastavitvev. Določi se lahko termin, ko naj se sinhronizacija izvede, perioda, indikator, če je sinhronizacija aktivna ali ne. Če se v okviru projekta ugotovi, da bi bilo smiselno dodati še kateri parameter, se ga v novi rešitvi določi in doda. Sinhronizacije se nato izvajajo skladno s temi nastavitvami.

Dnevnik opravil - v novi rešitvi se vzpostavi vmesnik z najmanj takimi funkcionalnostmi, kot jih ima modul dnevnik opravil v trenutni rešitvi. Ta pregledovalnik bo moral omogočati pregled, iskanje, filtriranje, razvrščanje po logih izvedenih akcij in opravil znotraj aplikacije. Trenuten pregledovalnik se v dogovoru z naročnikom nadgradi, da bo filter, razvrščanje in iskanje bilo uporabniku bolj prijazno (pregled zaloge vrednosti pri šifrantih aktivnosti, dodajanje atributov/parametrov za lažje iskanje).

Dnevnik sinhronizaciji - v novi rešitvi se vzpostavi vmesnik z najmanj takimi funkcionalnostmi, kot jih ima omenjeni modul v trenutni rešitvi. Ta pregledovalnik bo moral omogočati pregled, iskanje, filtriranje, razvrščanje po izvedenih sinhronizacijah aplikacije. Trenuten pregledovalnik se v dogovoru z naročnikom nadgradi, da bo filter, razvrščanje in iskanje bilo uporabniku bolj

prijazno (pregled zaloge vrednosti pri šifrantih aktivnosti, dodajanje atributov/parametrov za lažje iskanje).

Upravljanje z roki - v novi rešitvi se vzpostavi vmesnik z vsemi funkcionalnostmi, pravili in operacijami, ki so vezane na določanje, urejanje in upravljanje z roki, in sicer na način, kot so izvedene v trenutni rešitvi. Vzpostavi se možnost upravljanja z nastavitvami (vključno z upoštevanji nedelovnikov) ter pregledovanja in upravljanja z roki, ki so ustvarjeni v aplikaciji na podlagi izbranih pravil. Vnos in urejanje nedelovnikov se izvede v ločnem modulu oz. se dogovori z naročnikom v okviru projekta.

Obračunski interval - v novi rešitvi ni več potrebno vzpostavljati rešitve, s katero se je od izbranega trenutka dalje začel uporabljati 15 minutni obračunski interval. Vse nastavitve in pravila se v novi rešitvi vzpostavijo izključno za uporabo 15 minutnih obračunskih intervalov. Potrebno pa je ohraniti logiko, ki je v trenutni rešitvi pripravljena za ustrezno obvladovanje prehodov iz zimskega v letni čas ter obratno (prestopne ure). Tudi nova rešitev mora omogočiti vnos trenutkov prehoda med UTC+1 v UTC+2 ter obratno ter nato slednje pravilno upoštevati skozi vse funkcionalnosti rešitve.

Prevodi - rešitev mora podpirati večjezikovnost. Enako kot v obstoječi rešitvi se v ločenem modulu vzpostavi pregled podprtih jezikov ter zmožnost dodajanja novih. V tem modulu se lahko prenese dokument (v trenutni rešitvi v formatu xlsx), v kateri vsak stolpec predstavlja posamezni jezik, vsaka vrstica pa besedila, ukaze, nazive gumbov in vse entitete, za katere je znotraj aplikacije mogoče prilagoditi besedne prikaze. Prevode se ureja v izvoženem xlsx. Vsi popravki pa bodo po uvozu v aplikacijo nato vidni v vmesnikih aplikacije.

V trenutku aplikaciji se med nastavitvami nahajajo še trije moduli, tolerančni pas, formule za BO in EIP nastavitve. Nastavitvenega modula »Tolerančni pas« se v novi aplikaciji ne vzpostavi, pri modulih »Formule za BO« ter »Nastavitve EIP« pa se skupaj z naročnikom v okviru projekta preveri ustreznost delovanja ter po potrebi v novi rešitvi vzpostavi le tiste funkcionalnosti, ki jih bo naročnik določil kot smiselne.

Priloga A: Katalog poročil (osnutek)

V nadaljevanju je osnutek kataloga poročil, ki jih sistem IBIS++ ustvarja v okviru procesov BO/LPBO ter finančne poravnave. Končni seznam poročil, predlog, formatov in prejemnikov se potrdi v fazi analize na podlagi obstoječe rešitve in regulatornih zahtev.

ID	Naziv poročila	Proces	Prejemnik	Format	Podpisovan je	Jezik	Opombe
REP-BO-001	Poročilo kontrole sistema	BO	Skrbniki/operativ	XLSX	NE	SL	Kontrole in primerjave vhodnih podatkov

REP-BO-002	Poročilo povzetek BO	BO	Operativa, interne službe	XLSX	NE	SL/EN	Ključni rezultati obračuna
REP-BO-003	Poročilo za Agencijo	BO	Agencija (regulator)	XLSX + XML (TBD)	NE	SL	Vsebina skladno z veljavno predlogo
REP-BO-004	Poročilo ELES	BO	ELES	XLSX + XML (TBD)	NE	SL	Po dogovorjeni predlogi
REP-BO-005	Poročilo za FRS	BO	FRS	XLSX + XML (TBD)	NE	SL	Po dogovorjeni predlogi
REP-BO-006	Poročilo za člane (BO)	BO	Člani BS (Portal OT)	XLSX + XML	DA	SL/EN	Podpisano in objavljeno v zasebnem delu portala
REP-LPB-O-001	Kontrolna poročila LPBO	LPBO	Skrbniki/operativa	XLSX	NE	SL	Kontrole in primerjave vhodnih podatkov
REP-LPB-O-002	Poročilo povzetek LPBO	LPBO	Operativa, interne službe	XLSX	NE	SL/EN	Ključni rezultati letnega poročila
REP-LPB-O-003	Poročilo za člane (LPBO)	LPBO	Člani BS (Portal OT)	XLSX + XML	DA	SL/EN	Podpisano in objavljeno v zasebnem delu portala
FIN-001	Dokumenti za finančno poravnava	BO/LPBO	ERP/SAOP, DMS/SharePoint	PDF	DA (TBD)	SL	Ustvarjanje skladno z obstoječimi pravili in roki

	(POZ/NE G)						
AUD-001	Dnevnik izračuna in sledljivost (audit trail)	BO/LPB O	Skrbniki/audit	PDF/CSV (TBD)	NE	SL	Povezava vhodnih podatkov, različic in rezultatov
EXP-001	Izvoz podatkov v DWh	BO	DWh / analitika	API/CSV	NE	—	»Push« podatkov po dogovorjenem naboru

3.3. Nefunkcionalne zahteve (NFR)

ID	Zahteva	Prioriteta	Merilo / cilj
NFR-001	Skladnost s CGP podjetja	OBVEZNO	UI skladna z veljavnim priročnikom CGP; ključni tokovi potrjeni v UX pregledu.
NFR-002	Šifriranje dokumentov	OBVEZNO	TLS 1.2+ v prenosu; šifriranje v mirovanju (npr. AES) za dokumente in varnostne kopije; varno upravljanje ključev (HSM ali enakovredno).
NFR-003	Varnost dostopa	OBVEZNO	MFA za zunanje uporabnike; politike gesel/sej; zaklep računov; najmanjši potrebni privilegiji (least privilege).
NFR-004	Skladnost z GDPR	OBVEZNO	Podpora pravicam posameznikov; revizijska sled dostopov; hramba v EU/EGP; anonimizacija/izbris skladno s pravili.
NFR-005	Skalabilnost sistema	OBVEZNO	Arhitektura omogoča horizontalno/vertikalno skaliranje in rast obsega 15-minutnih meritev ter števila uporabnikov.
NFR-006	Razširljivost rešitve (Extensibility)	OBVEZNO	Modularna zasnova, API-centric, parametrizacija pravil in priprava na nove standarde.

NFR-007	Odzivni časi sistema	OBVEZNO	Za ključne uporabniške operacije 90 % zahtev < 3 s (ciljno); batch procesi v rokih, določenih z analizo.
NFR-008	Enotna prijava (SSO) in upravljanje identitet	OBVEZNO	SSO za interne uporabnike (Entra ID ali ekvivalent); MFA za zunanje; centralno upravljanje vlog in revizija.
NFR-009	Spletna dostopnost in podpora brskalnikom	OBVEZNO	Delovanje v sodobnih brskalnikih; odzivna zasnova; dosegljivost 24/7 v okviru SLA.
NFR-010	Večjezičnost uporabniškega vmesnika	OBVEZNO	Polna podpora vsaj za slovenščino in angleščino; upravljanje prevodov prek administracije.
NFR-011	Nadgradljivost in vzdrževanje (Maintainability)	OBVEZNO	Nadgradnje brez izgube podatkov/nastavitev; minimalni izpadi; redni varnostni popravki.
NFR-012	Razpoložljivost, neprekinjeno poslovanje in obnova delovanja (BC/DR)	OBVEZNO	Razpoložljivost $\geq 99,5$ %/mesec; RPO ≤ 15 min, RTO ≤ 4 h za kritične storitve; letni DR test.
NFR-013	Varnostne kopije, arhiviranje in preizkusi obnove	OBVEZNO	Dnevne kopije + inkrementalne skladno z RPO; šifriranje kopij; ločena hramba; četrtletni restore test.
NFR-014	Dnevniško beleženje dogodkov, nadzor in integracija s SIEM	OBVEZNO	Centralizirani dnevniki; integracija s SIEM; hramba varnostnih dnevnikov ≥ 12 mesecev; alarmi za ključne dogodke.
NFR-015	Varnostno testiranje, upravljanje ranljivosti in	OBVEZNO	SAST/dependency scanning; SBOM; letni penetracijski test; odprava kritičnih ranljivosti pred produkcijo.

	varna dobavna veriga		
NFR-016	Dostopnost za uporabnike (WCAG)	OBVEZNO	Cilj WCAG 2.1 AA za javni del; preverjanje ključnih tokov z avtomatskimi in ročnimi testi.

NFR-001 Skladnost s CGP podjetja

Prenova mora vključevati UX/UI izboljšave skladno z novo CGP. Izvajalec mora pri načrtovanju in izvedbi uporabniškega vmesnika (UI) sistema IBIS++ in spletnega portala OT v celoti upoštevati veljaven priročnik o celostni grafični podobi (CGP) naročnika. Cilj je zagotoviti vizualno skladnost nove rešitve z ostalimi digitalnimi kanali družbe Borzen ter uporabnikom ponuditi sodobno, intuitivno in pregledno okolje.

NFR-002 Šifriranje dokumentov in integracija z naročnikovim DMS

Rešitev mora zagotavljati šifriranje dokumentov v prenosu in v mirovanju. To pomeni, da mora biti celotna komunikacija med odjemalcem (uporabniškim brskalnikom ali drugo aplikacijo) in strežnikom aplikacije šifrirana (npr. preko protokola HTTPS/TLS), prav tako pa se morajo shranjeni dokumenti primarno voditi v naročnikovem sistemu za upravljanje z dokumenti (DMS), ki za namene integracije ponuja REST vmesnik; ponudnik mora pri izbiri šifrirnih standardov uporabiti široko dostopne in varnostno preverjene algoritme, ki so na trgu priznani kot varni (npr. TLS 1.2, ne TLS 1.1 in podobno).

Ta nefunkcionalna zahteva podpira strateški cilj informacijske varnosti na najbolj osnovni ravni - zagotavljanje zaupnosti dokumentov. Borzen upravlja z občutljivimi podatki, zato je šifriranje nujno, da se prepreči dostop nepooblaščenim osebam tudi v primeru varnostnega incidenta. Tehnični cilj visoke informacijske varnosti in zasebnosti je s tem neposredno naslovljen; varnostne mehanizme (kot je šifriranje) je treba vgraditi po načelu »security by design«. Poslovno gledano se s to zahtevo ščiti ugled in zaupanje v Borzen: s takšnimi ukrepi lahko družba partnerjem in strankam izkazuje, da resno jemlje varstvo podatkov, s čimer izpolnjuje tudi svojo skladnostno odgovornost in zmanjšuje tveganja (poslovni cilj obvladovanja tveganj).

NFR-003 Varnost dostopa

Poleg šifriranja je ključen vidik varnost dostopa: rešitev mora imeti mehanizme za močno avtentikacijo in avtorizacijo uporabnikov, skupaj z dodatnimi kontrolami prijav. Močna avtentikacija pomeni, da se uporabniki preverjajo z varnimi metodami - najmanj preko uporabniškega imena in kompleksnega gesla in dodatnega faktorja preverjanja (2FA), posebej za občutljive uporabniške vloge (skrbniki, potrjevalci).

Za notranje uporabnike Borzen mora rešitev zagotoviti integracijo z naročnikovim sistemom Active Directory, ki ga izvajalec lahko integrira neposredno, ali z uporabo Entra ID. Za zunanje uporabnike lahko rešitev zagotavlja lastno hrambo gesel ali drugo primerno metodo, ki pa mora upoštevati naročnikove standarde za gesla (kompleksnost, menjava ipd.).

Avtorizacija je že pokrita v funkcionalnih zahtevah; ta zahteva to nadgrajuje s tem, da mora biti upravljanje izvajano varno in centralno. Poleg tega mora sistem imeti nastavljeno avtomatsko odjavo uporabnikov po določenem času neaktivnosti - s tem se prepreči, da bi odprta seja predolgo ostala aktivna. Ta zahteva vključuje tudi omejevanje napačnih poskusov prijave - po 5 napačnih poskusih se račun začasno zaklene ali zahteva dodatno preverjanje, s čimer se preprečujejo napadi z ugibanjem gesel.

Podrobne zahteve bosta naročnik in izvajalec uskladili v podrobnem načrtovanju, mora pa izvajalec predpostavljati, da sistem izpolnjuje najboljše industrijske varnostne prakse za prijavne sisteme (»authentication systems«), vključno z beleženjem prijav (uspešnih in neuspešnih), zaščito pred CSRF pri spletnem vmesniku ipd.

Ta zahteva naslavlja pomemben del zahtev v sklopu NIS2/ZInfV-1, ISO 27001 in GDPR, ki definirajo, da je obvezno imeti politike močnih gesel, zaklepanja računov, preteka sej ipd.

NFR-004 Skladnost z GDPR

Sistem IBIS++ mora biti zasnovan po načelih vgrajene in privzete zasebnosti (privacy by design/default). Zagotavljati mora tehnično podporo za izpolnjevanje obveznosti po Splošni uredbi o varstvu podatkov (GDPR) in Zakonu o varstvu osebnih podatkov (ZVOP-2), kar vključuje varno obdelavo podatkov udeležencev trga, kontaktnih oseb in uporabnikov portala OT.

Ključni elementi zahteve:

- Uresničevanje pravic posameznikov: Sistem mora omogočati hiter priklic vseh osebnih podatkov, povezanih z določenim posameznikom (npr. uporabniški profil, kontaktni podatki v pogodbah, revizijske sledi). Omogočena mora biti trajna anonimizacija ali izbris podatkov ("pravica do pozabe"), razen v primerih, ko obstaja prevladujoča zakonska podlaga za hrambo (npr. po energetske ali finančni zakonodaji).
- Revizijska sled dostopa: Skladno z 22. členom ZVOP-2 mora sistem avtomatsko beležiti vsak vpogled, spremembo ali izbris osebnih podatkov. Revizijski dnevniki morajo biti nespremenljivi in omogočati identifikacijo osebe, ki je do podatkov dostopala, ter čas dostopa.
- Lokacija hrambe podatkov: Vsi podatki in njihove varnostne kopije se morajo nahajati na strežnikih znotraj EU/EGP. V primeru gostovanja v oblaku mora ponudnik jamčiti, da infrastruktura podizvajalca ne zapušča evropskega pravnega prostora.

NFR-005 Skalabilnost sistema

Sistem IBIS++ mora biti zasnovan skalabilno (horizontalno in vertikalno), kar omogoča nemoteno delovanje in visoko odzivnost tudi ob povečanju obsega podatkov in števila transakcij. Arhitektura mora omogočati dodajanje sistemskih virov brez posegov v jedro logiko aplikacije.

Ključni vidiki skalabilnosti:

- Rast števila in vrst PPM: Rešitev mora učinkovito obvladovati ob povečanju števila prevzemno-predajnih mest (PPM) ter uvajanje novih, kompleksnejših vrst PPM (npr. samooskrba, energetske skupnosti, prilagajanje odjema).
- Obdelava masovnih podatkov: Zaradi 15-minutnih obračunskih intervalov mora sistem omogočati procesiranje in hrambo povečanega obsega merilnih podatkov (»throughput«).
- Širitev uporabniške baze: Sistem mora podpirati morebitno povečanje števila članov bilančne sheme (OBS, OBPS) in povečan sočasen dostop zunanjih uporabnikov na portalu OT.
- Prilagodljivost virov: V primeru oblačne postavitve mora sistem podpirati dinamično dodeljevanje virov, v primeru lastne infrastrukture pa enostavno dodajanje aplikativnih in podatkovnih vozlišč.

NFR-006 Razširljivost rešitve (Extensibility)

Sistem IBIS++ mora biti zasnovan modularno, kar omogoča dodajanje novih funkcionalnosti, modulov ali integracijskih točk z minimalnimi posegi v obstoječe jedro sistema. Arhitektura mora podpirati evolucijo sistema v skladu s prihodnjimi spremembami tržnih pravil in tehnološkim napredkom.

Ključni elementi razširljivosti:

- Modularni izračunski motor (Calculation Engine): Arhitektura mora omogočati dodajanje novih izračunskih algoritmov ali spreminjanje obstoječih (npr. zaradi novih metodologij ACER/ENTSO-E) preko vtičnikov (plugins) ali konfiguracijskih skript, ne da bi bila potrebna ponovna izgradnja celotne aplikacije.
- API-centric arhitektura: Sistem mora temeljiti na standardiziranih in dokumentiranih API vmesnikih (npr. RESTful API), kar Borzenu omogoča, da v prihodnosti na IBIS++ enostavno poveže nove notranje ali zunanje sisteme (npr. platforme za prožnost, nove BI orodja).
- Parametrizacija namesto programiranja: Čim večje število poslovnih pravil, validacijskih shem in poročil mora biti nastavljenih preko administrativnega vmesnika (konfiguracija), namesto da bi bili trdo kodirani v programski opremi.
- Podpora novim standardom: Rešitev mora biti pripravljena na razširitev z novimi podatkovnimi standardi (npr. prehod na nove verzije CIM standarda ali uvedbo kodeksa za fleksibilnost), kar vključuje fleksibilno metapodatkovno strukturo.
- Razširljivost portala OT: Spletni portal mora omogočati dodajanje novih vsebinskih sklopov ali nadzornih plošč (dashboards) za člane bilančne sheme.

NFR-007 Odzivni časi sistema

Uporabniška izkušnja sistema IBIS++ in portala OT mora biti odzivna in tekoča. Sistem mora zagotavljati hitro procesiranje zahtevkov, ki ne ovira delovnih procesov zaposlenih na Borzenu in zunanjih članov bilančne sheme, kar v praksi pomeni, da sem mora > 80% zahtev obdelati v manj kot 2 sekundah, > 95% pa v manj kot 4 sekundah.

Ključni parametri odzivnosti:

- Tipične operacije: odzivni čas za vsaj 95 % zahtevkov mora biti krajši od 4 sekund. To vključuje prijave, navigacijo po menujih, iskanje in filtriranje v seznamih (npr. pregled pogodb, finančnih kritij ali partnerjev) ter odpiranje dokumentov.
- Zahtevne operacije: masovni uvozi merilnih podatkov (DO/SO meritve) ter zagoni kompleksnih izračunov (BO in LPBO) lahko trajajo dlje (več minut), vendar morajo potekati v ozadju in ne smejo blokirati uporabniškega vmesnika.
- Indeksiranje in optimizacija: za ohranjanje odzivnosti pri delu z velikimi bazami podatkov (npr. 15-minutne meritve za PPM) mora sistem uporabljati napredno indeksiranje in optimizirane API klice.
- Konsistentnost pod obremenitvijo: predpisani odzivni časi morajo ostati stabilni tudi ob polni obremenitvi sistema in sočasnem dostopu večjega števila uporabnikov na portalu OT.

NFR-008 Enotna prijava (SSO) in upravljanje identitet

Sistem IBIS++ mora podpirati sodobne in varne mehanizme avtentikacije. Za zaposlene naročnika mora biti omogočena enotna prijava (SSO) z naročnikovim Active Directory (lahko neposredno, ali preko Entra ID), za zunanje uporabnike (člane bilančne sheme) na portalu OT pa prehod na varno prijavo z uporabo dvo-faktorske avtentikacije (2FA).

Ključni elementi zahteve:

- Integracija z Microsoft Entra ID (Azure AD) za zaposlene: Za interne uporabnike mora sistem podpirati avtentikacijo preko protokola OAuth2 ali OpenID Connect. Omogočena mora biti brezšivna prijava, ki prepozna obstoječo sejo v delovnem okolju Microsoft 365.
- 2FA z Microsoft Authenticatorjem za zunanje uporabnike: Za dostop do portala OT se namesto digitalnih potrdil uvede prijava z uporabniškim imenom in geslom, ki je obvezno nadgrajena z drugim faktorjem preko aplikacije Microsoft Authenticator (odobritev obvestila/push notification ali vnos časovne kode).
- Upravljanje zunanjih identitet: Sistem mora omogočati varno registracijo zunanjih uporabnikov in enostaven postopek povezave (pairing) njihovega računa z aplikacijo MS Authenticator.
- Centralizirano varnostno upravljanje: Sistem mora podpirati uveljavljanje varnostnih politik (npr. zahteva po ponovni avtentikaciji po določenem času neaktivnosti ali ob dostopu iz neznanih IP naslovov), ki se centralno upravljajo preko naročnikovega identitetnega sistema.
- Preklic dostopa: Ob izbrisu ali deaktivaciji uporabnika v centralnem imeniku ali na zahtevo skrbnika mora biti dostop do vseh delov sistema (IBIS in portal OT) onemogočen takoj.

NFR-009 Spletna dostopnost in podpora brskalnikom

Sistem IBIS++ in portal OT morata biti v celoti dostopna prek sodobnega spletnega vmesnika, ki omogoča varno in nemoteno delo od koderkoli, brez potrebe po nameščanju namenske programske opreme na delovne postaje.

Ključni elementi zahteve:

- Podpora brskalnikom: Vmesnik mora brezhibno delovati v vseh sodobnih spletnih brskalnikih, ki imajo v času oddaje ponudbe več kot 5-odstotni tržni delež (npr. Chrome, Edge, Firefox, Safari).
- Stalna dosegljivost: Sistem mora biti v okviru dogovorjene razpoložljivosti dostopen 24/7 prek vseh tipov internetnih povezav.
- Odzivna zasnova (RWD): Uporabniški vmesnik mora biti optimiziran za različne ločljivosti zaslonov, kar zagotavlja preglednost podatkov tako na namiznih računalnikih kot na prenosnih napravah.
- Enostavna uporaba: Vmesnik mora biti intuitiven, kar zmanjšuje potrebo po obsežnem usposabljanju in povečuje agilnost zaposlenih ter zunanjih uporabnikov.

NFR-010 Večjezičnost uporabniškega vmesnika

Uporabniški vmesnik sistema IBIS++ in portala OT mora podpirati večjezičnost. Sistem mora omogočati popolno lokalizacijo vsebine in funkcionalnih elementov.

Ključni elementi zahteve:

- Podprta jezika: Obvezna je polna podpora za slovenski in angleški jezik.
- Izbira jezika: Uporabnik mora imeti možnost enostavne menjave jezika neposredno v vmesniku, sistem pa si mora to nastavitvev zapomniti za prihodnje prijave.
- Obseg prevodov: Večjezičnost mora vključevati vse menije, gumbe, sistemska obvestila, napake, opise polj ter ključne statuse in poročila.
- Tuji deležniki: Podpora angleškemu jeziku je ključna za tuje člane bilančne sheme, ki poslujejo na slovenskem trgu z električno energijo.

NFR-011 Nadgradljivost in vzdrževanje (Maintainability)

Sistem IBIS++ mora omogočati redno posodabljanje in nadgradnje na nove različice brez tveganja za izgubo podatkov, nastavitvev ali prilagoditev. Arhitektura mora zagotavljati dolgoročno tehnološko vzdržnost in hitro uvažanje varnostnih popravkov.

V okviru vzdrževanja mora ponudnik redne nadgradnje / implementacije varnostnih posodobitev predvideti kot del preventivnega vzdrževanja, ki mora biti del pogodbenega pavsala, pri čemer mora namestitvev kritičnih popravkov zagotoviti v največ 72 urah.

Ključni elementi zahteve:

- Združljivost za nazaj: Nadgradnje jedra sistema ne smejo vplivati na obstoječe izračunske algoritme, zgodovinske podatke bilančnega obračuna ali integracijske vmesnike (API).
- Minimalni izpadi: Posodobitve in vzdrževalna dela se morajo izvajati z minimalnim časom nedostopnosti, praviloma izven konic tržnega poslovanja in vnaprej napovedanih terminih.
- Varnostni popravki: Ponudnik mora zagotoviti redno nameščanje varnostnih popravkov za vse komponente rešitve (aplikativni del, podatkovna baza, spletni strežnik) v najkrajšem možnem času po odkritju ranljivosti.
- Skladnost s standardi: Redno posodabljanje je nujno za ohranjanje skladnosti z direktivo NIS2 (upravljanje ranljivosti) in standardom ISO 27001, ki od Borzena zahtevata uporabo podprte in varne programske opreme.

NFR-012 Razpoložljivost, neprekinjeno poslovanje in obnova delovanja (BC/DR)

Sistem IBIS++ (Portal OT, API storitve in podatkovna plast) mora zagotavljati visoko razpoložljivost ter možnost hitre in nadzorovane obnove delovanja v primeru izpada, incidenta ali izgube podatkov. Rešitev mora omogočati izvajanje ključnih poslovnih procesov (zlasti BO/LPBO) v dogovorjenih časovnih okvirih tudi ob motnjah.

Ključni elementi zahteve:

- Razpoložljivost: Ciljna razpoložljivost produkcijskega sistema je najmanj 99,5 % na mesečni ravni (brez vnaprej napovedanih vzdrževalnih oken).
- RPO/RTO: Rešitev mora podpirati cilje obnove vsaj $RPO \leq 15$ minut in $RTO \leq 4$ ure za kritične funkcionalnosti (API, dostop do podatkov, generiranje in dostop do poročil). Končne vrednosti se potrdijo v fazi analize glede na poslovne roke in oceno tveganj.
- Redundanca in odprava posameznih točk odpovedi: Kritične komponente (podatkovna baza, aplikacijski strežniki, repozitorij dokumentov) morajo biti zasnovane brez posamezne točke odpovedi ter omogočati preklap (failover) na sekundarno instanco v dogovorjenem času.
- Vzdrževalna okna: Vzdrževalna dela se izvajajo izven kritičnih poslovnih obdobj in so vnaprej napovedana; za nujne varnostne posege mora biti opredeljen pospešeni postopek obveščanja in odobritve.
- Preizkusi DR: Najmanj enkrat letno se izvede preizkus obnovitve (DR test), ki vključuje obnovo iz varnostnih kopij in osnovni funkcionalni preizkus; rezultat se dokumentira v poročilu z ukrepi za izboljšave.

NFR-013 Varnostne kopije, arhiviranje in preizkusi obnove

Rešitev mora zagotavljati avtomatizirano izdelavo varnostnih kopij podatkovnih baz, konfiguracij in dokumentnega repozitorija ter definirano politiko hrambe in arhiviranja. Varnostne kopije morajo biti šifrirane in redno preizkušene z obnovitvenimi postopki.

Ključni elementi zahteve:

- Obseg kopij: V varnostne kopije morajo biti vključene podatkovne baze, konfiguracije aplikacije in integracij, repozitorij dokumentov pa mora biti hranjen v DMS, ki se redno nadgrajuje.
- Frekvenca: Minimalno dnevna polna kopija in redne inkrementalne kopije (pogostost se uskladi z zahtevanim RPO).
- Hramba: Politika hrambe mora ločiti kratkoročno hrambo za operativno obnovo (npr. 30 dni) in dolgoročno arhivsko hrambo (npr. 12 mesecev ali skladno z internimi pravili naročnika).
- Varnost kopij: Varnostne kopije morajo biti šifrirane, dostop do njih pa omejen in revizijsko sledljiv. Kopije se hranijo ločeno od primarnega okolja (logična in po potrebi lokacijska ločitev).
- Preizkusi obnove: Najmanj enkrat na četrletje se izvede preizkus obnove iz varnostnih kopij (restore test) in dokumentira rezultat.

NFR-014 Dnevniško beleženje dogodkov, nadzor in integracija s SIEM

Sistem mora zagotavljati celovito beleženje (logging) in nadzor (monitoring) delovanja ter varnostnih dogodkov. Dnevniki morajo omogočati sledljivost poslovnih transakcij, odkrivanje anomalij in podporo preiskavam incidentov, hkrati pa morajo biti integrabilni v naročnikov centralni sistem za nadzor in/ali SIEM.

Ključni elementi zahteve:

- Centralizirani dnevniki: Aplikacija in portal morata beležiti dogodke v centralni dnevniški sistem (npr. log aggregator), z uporabo korelacijskih identifikatorjev (correlation ID) za sledenje zahtevkom prek integracij.
- Varnostni dogodki: Beležiti je treba prijave/odjave, neuspešne prijave, spremembe pravic, vpoglede v osebne podatke in dokumente, ter kritične administrativne posege.
- Integracija s SIEM: Dnevniki morajo biti izvozni v standardnem formatu (npr. syslog/CEF/JSON) in integrabilni v SIEM naročnika; podprti morajo biti osnovni alarmni scenariji (npr. več zaporednih neuspešnih prijav, nenavadna aktivnost skrbniških računov).
- Hramba dnevnikov: Minimalna hramba varnostnih dnevnikov je 12 mesecev (ali skladno z internimi pravili naročnika); dnevniki morajo biti zaščiteni pred spremembami.
- Nadzor razpoložljivosti in zmogljivosti: Sistem mora omogočati nadzor ključnih metrik (odzivni časi, napake, zasedenost virov, čakalne vrste, integracijske napake) in obveščanje ob prekoračitvah pragov.

NFR-015 Varnostno testiranje, upravljanje ranljivosti in varna dobavna veriga

Rešitev mora biti razvita in vzdrževana skladno z načeli varnega razvoja. Vključevati mora redno varnostno testiranje, upravljanje ranljivosti in nadzor odvisnosti (third-party risk), vključno z obvladovanjem CVE in dobavno verigo programske opreme.

Ključni elementi zahteve:

- Varnostni pregledi kode in odvisnosti: V razvojnem procesu se izvajajo SAST, pregled odvisnosti (dependency scanning) in po potrebi DAST. Izvajalec mora zagotoviti odpravo kritičnih ranljivosti pred produkcijskim zagonom.
- SBOM: Za ključne komponente rešitve se pripravi SBOM (seznam programskih komponent) in proces spremljanja ranljivosti komponent skozi življenjski cikel.
- Penetracijski testi: Pred produkcijskim zagonom in nato najmanj enkrat letno se izvede neodvisno penetracijsko testiranje; ugotovitve se odpravijo v dogovorjenih rokih glede na kritičnost.
- Upravljanje popravkov: Izvajalec mora zagotavljati redno nameščanje varnostnih popravkov in obveščanje naročnika o kritičnih ranljivostih ter predlaganih ukrepih.

NFR-016 Dostopnost za uporabnike (WCAG)

Portal OT (zlasti javni del in ključni uporabniški procesi) mora biti zasnovan tako, da je dostopen uporabnikom z različnimi oviranostmi. Dostopnost se upošteva pri načrtovanju, razvoju in testiranju uporabniškega vmesnika.

Ključni elementi zahteve:

- Standard: Cilj je skladnost vsaj z WCAG 2.1 na ravni AA za javni del portala; v uporabniškem delu se isti nivo upošteva za ključne obrazce in vsebine.
- Praktične zahteve: Podpora tipkovnici, ustrezni kontrasti, smiselna struktura naslovov, besedilne alternative (alt) za slike ter pravilna raba ARIA atributov tam, kjer je potrebno.
- Testiranje: Dostopnost se preverja z avtomatskimi orodji in ročnimi preizkusi na ključnih uporabniških tokovih (npr. izpolnjevanje vloge, prijava, prenos dokumentov).

4. Tehnične zahteve

4.1. Obstoječe stanje

Trenutna informacijska rešitev je sestavljena iz:

- Portal OT (DNN + AngularJS moduli),
- Backend (API, poslovna logika, .NET, Dapper),
- Podatkovna baza MS SQL,

- Namenska IBIS++ WPF aplikacija.

4.2. Ciljna arhitektura

Ciljna arhitektura ohranja 3-nivojski model:

- podatkovni strežnik,
- aplikacijski strežnik (API),
- frontend.

Frontend se izdelava v Angular (zadnja LTS). Izvajalec lahko predlaga alternativo DNN, če zagotovi večjo varnost, vzdrževanje in dolgoročno podporo, vendar mora alternativa še zmeraj teči v okviru naročnikovega upravljanega okolja (Microsoft Windows strežniki, .NET ogrodje). Arhitektura mora slediti najboljšim praksam izbranih tehnologij in priporočilom primarnih proizvajalcev.

- Angular zadnja LTS,
- .NET zadnja LTS (za API razširitve),
- MS SQL 2019+,
- TLS 1.2+,
- Git CI/CD,
- Kompatibilnost z obstoječimi API-ji.

Tehnologije ne smejo imeti aktivnih CVE ranljivosti.

4.3. Integracije in vmesniki

Izvajalec mora zagotoviti kompatibilnost z obstoječimi integracijami ter pripraviti integracijsko dokumentacijo (ICD - Interface Control Document) za vse zunanje sisteme. ICD mora vsebovati najmanj: opis namena integracije, smer prenosa podatkov, seznam podatkovnih elementov in metapodatkov, format (npr. XML/JSON/CSV), protokol (REST/SOAP/SFTP), avtentikacijo in avtorizacijo, pravila verzioniranja, mehanizme ponavljanja (retry), idempotentnost, obravnavo napak (error codes), časovne roke (SLA) ter način nadzora in dnevniškega beleženja.

Za nove ali prenovljene API vmesnike mora izvajalec pripraviti OpenAPI specifikacijo (OpenAPI 3.x) in zagotoviti verzioniranje, ki ne prekine obstoječih odjemalcev (backwards compatibility), razen če je drugače izrecno dogovorjeno z naročnikom.

Sistem / integracija	Namen (podatki)	Smer	Vmesnik / format	Avtentikacija in varnost	Opombe (napake, pogostost)

MDM	Partnerji in kontakti (matični podatki, vloge kontaktov)	MDM → IBIS++ / IBIS++ → MDM	API ali paketna sinhronizacija; JSON/XML	TLS; avtorizacija na ravni storitve	MDM je izvor resnice; sinhronizacija po urniku in/ali na zahtevo
ERP / SAOP	Računovodski podatki, fakture, izpisi; potrjevanje dokumentov	IBIS++ ↔ ERP	API/SOAP/DB integracija (TBD)	TLS; servisni računi; revizijska sled	Ohranitev obstoječih procesov; dogovor o idempotentnosti
SharePoint	Hramba dokumentov (vloge, poročila, priloge, metapodatki)	IBIS++ → SharePoint	REST/Graph API; PDF	TLS; servisni račun; šifriranje	Metapodatki in pravice po dogovorjenih pravilih; podpira verzioniranje
DMS	Hramba dokumentov (vloge, poročila, priloge, metapodatki)	IBIS++ → DMS	REST API	TLS; servisni račun; šifriranje	Metapodatki in pravice po dogovorjenih pravilih; podpira verzioniranje
EIP	Elektronska izmenjava podatkov in objave poročil	IBIS++ ↔ EIP	Spletni servis; XML/CSV/PDF (TBD)	TLS; podpisovanje sporočil, kjer je zahtevano	Ohraniti obstoječe sheme in roke objav
SMTP / e-pošta	Obveščanje uporabnikov in opomniki	IBIS++ → SMTP	SMTP	TLS; SPF/DKIM/DMARC po naročnikovih pravilih	Čakalne vrste; ponavljanje pošiljanja; evidenca poslanih sporočil
Identity provider	SSO/MFA (Entra ID ali ekvivalent)	IdP → IBIS++	OIDC/SAML (TBD)	MFA; pogoji dostopa; politike sej	Ločeni tokovi za interne in zunanje uporabnike
DWH / BI	Izvoz podatkov za analitiko in poročanje	IBIS++ → DWH	ETL/API; JSON/CSV (TBD)	TLS; servisni račun; minimalni privilegiji	Dogovor o osveževanju in konsistentnosti podatkov

Pri prenosu dokumentov v DMS/SharePoint mora sistem poleg datotek prenesti tudi metapodatke. Minimalni nabor metapodatkov obsega npr. identifikator sporočila (messageld), identifikator partnerja (EIC), številko dokumenta/računa, datum dokumenta, tip dokumenta (POZ/NEG), znesek ter obdobje obračuna. Končni seznam metapodatkov in mapiranje polj se potrdi v vzpostavitveni dokumentaciji na podlagi obstoječe integracije.

5. Načrt implementacija in vzdrževanje

Implementacija sistema IBIS++ bo temeljila na tehnološki posodobitvi (refaktoringu) preverjene poslovne logike obstoječega sistema. Ključni poudarek bo na prehodu v sodobno, varno arhitekturo, odpravi kritičnih varnostnih vrzeli ter izboljšanju uporabniške izkušnje ob ohranitvi integritete izračunov bilančnega obračuna.

5.1. Faze implementacije rešitve

5.1.1. Faza 1: Analiza vrzeli in varnostna revizija

Analiza razlik (Gap Analysis): Identifikacija ključnih razlik med obstoječo rešitvijo in novimi zahtevami.

Varnostna diagnoza: Natančen popis varnostnih pomanjkljivosti trenutnega sistema in priprava načrta za njihovo sistemsko odpravo.

Arhitekturni načrt: Specifikacija novega tehnološkega sklada, ki bo podpiral 2FA avtentikacijo in strožje varnostne protokole.

Tehnična specifikacija: Priprava dokumenta podrobne arhitekture sistema, podatkovnega modela in načrta integracij (API specifikacije).

Načrt kakovosti in testiranja: Opredelitev testnih scenarijev in pogojev za prehod v naslednje faze.

5.1.2. Faza 2: Razvoj refaktoring in konfiguracija

Vzpostavitev okolij: Priprava razvojnega, testnega in produkcijskega okolja.

Razvojni refaktoring in varnostno utrjevanje

Migracija in posodobitev kode: Prenos obstoječe poslovne logike v sodobno ogrodje (npr. .NET Core, Angular/React) ob hkratni odpravi zastarelih in ranljivih knjižnic.

Implementacija varne prijave: Vzpostavitev 2FA z aplikacijo Microsoft Authenticator za zunanje uporabnike in SSO za zaposlene.

Implementacija integracij: Povezava z ERP sistemom, MDM in drugimi zunanjimi viri podatkov.

Varnostno utrjevanje (Hardening): Implementacija zaščite pred napadi (SQLi, XSS), prenova sistema šifriranja podatkov in vzpostavitev nespremenljive revizijske sledi.

5.1.3. Faza 3: Testiranje in zagotavljanje kakovosti

Primerjalno testiranje (Regression Testing): Preverjanje, ali refaktorirani algoritmi dajejo rezultate, ki so identični obstoječemu sistemu.

Uporabniško sprejemno testiranje (SAT): Testiranje portala OT in zalednega sistema s strani ključnih uporabnikov na realnih podatkih.

Penetracijski testi: Izvedba neodvisnih varnostnih testov za potrditev, da so bile ugotovljene varnostne vrzeli uspešno zaprte.

Varnostno testiranje: Izvedba penetracijskih testov in preverjanje skladnosti z NIS2/ISO 27001.

5.1.4. Faza 4: Migracija podatkov in šolanje

Migracija baze podatkov: Prenos zgodovinskih podatkov v novo, optimizirano strukturo ob hkratnem čiščenju in validaciji podatkov.

Usposabljanje: Šolanje zaposlenih in priprava navodil za zunanje uporabnike glede novega načina prijave (2FA).

5.1.5. Faza 5: Vzporedni tek in produkcijski zagon

Vzporedni tek (Shadow Run): Obdobje, ko sistem IBIS++ deluje vzporedno s starim sistemom, da se s primerjavo rezultatov dokončno potrdi pravilnost izračunov.

Preklop (Go-Live): Uradni prehod na produkcijsko delovanje novega sistema. Prehod v fazo vzdrževanja in podpore.

5.2. Časovni načrt implementacije

Faza projekta	Trajanje	Ključni mejnik (Milestone)
Faza 1: Analiza in varnostna revizija	1,5 meseca	Potrjen načrt odprave varnostnih vrzeli in specifikacija razlik.
Faza 2: Razvojni refactoring in 2FA	4,5 meseca	Zaključena migracija kode in implementacija varnostnih modulov.
Faza 3: Varnostno in SAT testiranje	2 meseca	Uspešno opravljeni penetracijski testi in uporabniški testi.
Faza 4: Migracija in šolanje	1 meseca	Pripravljenost uporabnikov in migrirana baza podatkov.
Faza 5: Vzporedni tek in Go-Live	1 mesec	Potrjena skladnost izračunov in uradni zagon.
Skupaj do zagona	10 mesecev	Primopredaja varnega in posodobljenega sistema.

Po uspešno zaključenem poskusnem obratovanju in podpisu končnega prevzemnega zapisnika rešitev preide v redno fazo vzdrževanja.

5.3. Prehod v fazo vzdrževanja in podpore

5.3.1. Garancijsko vzdrževanje

Izvajalec po zagonu zagotavlja garancijsko dobo, kot določeno v osnutku pogodbe, v kateri brezplačno odpravlja vse napake, ki so posledica neskladnosti s potrjeno specifikacijo.

5.3.2. Redno vzdrževanje in SLA (Service Level Agreement)

Podpora uporabnikom: Vzpostavitev enotne točke za prijavo težav (Helpdesk) s predpisanimi odzivnimi časi glede na kritičnost napake (skladno z osnutkom pogodbe).

Preventivno vzdrževanje: Redni pregledi baz podatkov, optimizacija poizvedb in spremljanje zmogljivosti.

Varnostne posodobitve: Redno nameščanje popravkov za operacijske sisteme in aplikativne komponente.

5.3.3. Prilagoditveno in razvojno vzdrževanje

Sistem IBIS++ se bo v fazi vzdrževanja prilagajal novim evropskim in nacionalnim regulatornim zahtevam (npr. spremembe ENTSO-E kodeksov). Za večje nadgradnje se uporablja postopek upravljanja sprememb (Change Management), ki zagotavlja, da nove funkcije ne ogrozijo stabilnosti obstoječega obračuna.

5.4. Primopredaja dokumentacije

Ob prehodu v vzdrževanje izvajalec preda posodobljeno administratorsko in uporabniško dokumentacijo ter kodo (v skladu s pogodbenimi določili), kar naročniku zagotavlja dolgoročno neodvisnost in varnost delovanje rešitve.

6. Upravljanje projekta

Upravljanje projekta mora zagotavljati pregledno izvedbo, sledljivost odločitev in sprememb ter obvladovanje tveganj in kakovosti skozi celoten življenjski cikel rešitve. Projekt se izvaja po fazah, opisanih v tem poglavju, pri čemer se lahko posamezne funkcionalnosti dobavljajo iterativno (npr. po sklopih oziroma iteracijah), če je to smiselno glede na poslovne prioritete.

Projektno upravljanje mora biti usklajeno z notranjimi akti naročnika, zlasti glede ločitve okolij, upravljanja dostopov, dokumentiranja, testiranja ter odobritev sprememb in prehodov v produkcijo. Izvajalec mora naročniku omogočiti vpogled v projektne evidence ter dokazila (npr. status poročila, registre, poročila testiranja) in sodelovati pri morebitnih notranjih ali zunanjih presojah. Ključna dokumentacija za upravljanje dokumenta vsebuje vsaj:

- projektni načrt (obseg, pristop izvedbe, terminski plan, viri, komunikacija, načrt kakovosti, načrt testiranja, načrt migracije in uvajanja);
- register zahtev in sledljivosti (zahteva → implementacija → test);

- register tveganj (opis, ocena verjetnosti in vpliva, raven tveganja, lastnik, ukrepi, roki in status);
- register odprtih vprašanj in odločitev (issue log / decision log);
- register sprememb (zahtevki za spremembo) ter evidenca odobritev.

Upravljanje tveganj se izvaja sproti: izvajalec mora tveganja prepoznati, oceniti in obravnavati (z ukrepi za zmanjšanje verjetnosti ali vpliva) ter jih redno usklajevati z naročnikom. Kritična tveganja oziroma odstopanja od terminskega plana je potrebno nemudoma eskalirati na projektno vodstvo oziroma projektni odbor.

Če izvajalec pri izvedbi uporablja podizvajalce, mora zanje (ali za njihovo zamenjavo) pridobiti predhodno soglasje naročnika ter zagotoviti, da podizvajalci izpolnjujejo enake zahteve glede varnosti, zaupnosti, kakovosti, dokumentiranja in sledljivosti kot glavni izvajalec. Podizvajalci, ki so prijavljeni kot del originalne ponudbe se obravnavajo skladno z ZJN-3 in ocenjujejo kot del originalnega postopka, zato za njih posebno ukrepanje ni potrebno.

6.1. Projektno vodenje

Naročnik in izvajalec imenujeta vodji projekta, ki sta odgovorna za operativno vodenje, koordinacijo aktivnosti, spremljanje terminskega plana ter redno poročanje; za potrjevanje ključnih odločitev in mejnikov naročnik praviloma vzpostavi projektni odbor (usmerjevalni odbor).

Ključne vloge, ki so v okviru projektnega vodenja definirane in jih zagotovi naročnik so:

- vodja projekta naročnika: koordinacija naročnikovih deležnikov, organizacija potrjevanj in eskalacij;
- tehnični vodja/arhitekt izvajalca: tehnične odločitve, arhitektura, integracije in nadzor kakovosti izvedbe;
- vodja testiranja: priprava in izvedba testnega načrta, vodenje evidence napak in potrditev odprave;
- ključni uporabniki naročnika: sodelovanje pri potrjevanju zahtev in izvedbi uporabniškega sprejemnega testiranja (UAT).

Izvajalec zagotovi redne dokaze napredka (npr. ob zaključku posameznih iteracij ali funkcionalnih sklopov) ter sprotno usklajuje odprta vprašanja. Minimalna struktura koordinacije praviloma vključuje: začetni sestanek (kick-off), tedenske operativne sestanke projektne skupine ter periodične (npr. mesečne) sestanke projektnega odbora. O sestankih se vodijo zapisniki, ki vsebujejo sprejete odločitve, naloge, roke in odgovorne osebe. Za vodenje zahtev, nalog, hroščev in sprememb se uporabi dogovorjeno orodje (ki ga zagotovi naročnik), ki omogoča sledljivost in revizijsko sled. Projektna dokumentacija se vodi v centralnem repozitoriju naročnika z verzioniranjem in urejenimi pravicami dostopa.

6.2. Razmejitev dokumentacije

Dokumentacija je ključni del dobave in je pogoj za prevzem posameznih faz ter za prehod v produkcijo. Pripravlja se sproti skozi celoten življenjski cikel projekta, je verzionirana (oznaka verzije in datum) ter shranjena v centralnem repozitoriju naročnika z urejenimi pravicami dostopa.

Izvajalec pripravi in predloži najmanj naslednjo dokumentacijo, naročnik pa jo pregleda in potrdi v okviru dogovorjenih potrditvenih točk:

- projektna dokumentacija: projektni načrt, terminski plan (Gantt), načrt komunikacije, načrt kakovosti, načrt testiranja, načrt migracije in uvajanja;
- dokumentacija podrobne analize: poročilo o analizi vrzeli, popis in prioritizacija zahtev, sledljivost zahtev;
- tehnična dokumentacija: arhitektura (diagrami komponent), omrežna/topološka umeščenost, podatkovni model, specifikacije integracij (API), seznam tehnologij in verzij;
- varnostna dokumentacija: opis varnostnih kontrol (avtentikacija, avtorizacija, šifriranje, beleženje), ocena tveganj in utemeljitve morebitnih sprejetih tveganj, poročila varnostnih testov;
- dokumentacija testiranja: testni načrti in scenariji, rezultati testov, evidence napak in potrditev odprave, zapisniki UAT;
- dokumentacija migracije: mapiranje podatkov, pravila validacije, poročila o migraciji in o preverjanju pravilnosti izračunov;
- operativna dokumentacija (runbook): namestitve, konfiguracija, postopki uvedbe in povrnitve (deployment/rollback), varnostno kopiranje in obnova, monitoring, administrativni postopki;
- uporabniška dokumentacija in gradiva za usposabljanje (za interne in zunanje uporabnike);
- izročitev izvorne kode, konfiguracij in (kjer je relevantno) evidence odvisnosti/komponent (npr. SBOM) ter licenčnih obveznosti.

Dokumentacija se posodablja ob vsaki spremembi, ki vpliva na delovanje ali konfiguracijo sistema. Sprememba se ne šteje za v celoti zaključeno, dokler niso posodobljeni tudi ustrezni deli dokumentacije.

6.3. Potrjevanje izdelkov in časovni roki

Potrjevanje (prevzem) se izvaja etapno: naročnik potrjuje ključne dokumente, dobave funkcionalnosti ter zaključke testiranja, in sicer na podlagi vnaprej dogovorjenih meril ter predloženih dokazil (npr. testna poročila, zapisniki, verzionirane dobave). Potrditve se dokumentirajo in so del revizijske sledi projekta.

Postopek potrjevanja posameznega izdelka praviloma poteka v naslednjih korakih:

- izvajalec izdelek preda v dogovorjeni obliki in repozitoriju ter ga označi z verzijo;
- naročnik izvede pregled in poda pripombe oziroma potrdi skladnost;
- izvajalec odpravi pripombe in ponovno predloži izdelek;

- naročnik izdelek potrdi (npr. s podpisom prevzemnega zapisnika ali z elektronsko potrditvijo).

Roki za pregled in potrditev se določijo v projektnem načrtu. Naročnik praviloma poda pripombe v razumnem roku (npr. 7-10 delovnih dni), pri obsežnejših dobavah ali v času odsotnosti ključnih deležnikov pa se rok uskladi. Izvajalec mora pripombe obravnavati prednostno in predlagati rok odprave, tako da se ne ogrozi doseganje ključnih mejnikov.

Kot merila za potrditev se med drugim upoštevajo: skladnost s potrjenimi zahtevami, uspešno izvedena dogovorjena testiranja, odsotnost kritičnih napak, posodobljena dokumentacija ter (kjer je relevantno) odobritev spremembe v skladu s postopkom upravljanja sprememb.

6.4. Upravljanje sprememb

Upravljanje sprememb poteka kontrolirano in sledljivo, v skladu z notranjim pravilnikom naročnika o upravljanju sprememb. Vse spremembe (zahtev, obsega, arhitekture, konfiguracij, integracij, migracijskih pravil ter spremembe v produkcijskem okolju) se obravnavajo na podlagi zahtevka za spremembo, ki je evidentiran v dogovorjenem orodju.

Zahtevek za spremembo mora praviloma vsebovati vsaj:

- opis spremembe in razlog/poslovno utemeljitev;
- oceno vplivov (funkcionalni vpliv, vpliv na varnost, vpliv na integracije, vpliv na podatke in uporabnike);
- oceno tveganj (verjetnost/vpliv) ter predlagane ukrepe za njihovo obvladovanje;
- oceno napora, stroškov in vpliva na terminski plan;
- predlog izvedbe, vključno z načrtom testiranja ter načrtom uvedbe in povrnitve (deployment/rollback);
- predlog termina izvedbe in načrt komunikacije.

Spremembe se razvrščajo glede na vpliv in nujnost (npr. standardne, redne in nujne/izredne). Nujne spremembe so dovoljene le, če je treba nemudoma odpraviti kritično napako ali varnostno ranljivost oziroma zagotoviti neprekinjeno poslovanje; tudi v tem primeru mora izvajalec zagotoviti ustrezno dokumentiranje, naknadno potrjevanje in presojo učinkov.

Spremembe, ki vplivajo na produkcijo, so dovoljene šele po uspešnem testiranju v testnem okolju, odpravi kritičnih napak in pridobitvi vseh potrebnih odobritev. Izvajalec spremembe ne sme uvesti brez izrecnega soglasja naročnika oziroma pristojnega kolegijskega upravljanja sprememb.

Vsaka sprememba mora imeti dokazila o izvedenem testiranju in mora vključevati posodobitev dokumentacije. Zaključek spremembe se evidentira v registru sprememb skupaj z odobritvami, rezultati testov in datumom uvedbe.

6.5. Glavni mejniki

V nadaljevanju so navedeni glavni mejniki projekta, izraženi v mesecih od podpisa pogodbe (M+0).

Mejnik	Opis mejnika	Ključni rezultati / dokazila
M+0	Podpis pogodbe in zagon projekta (kick-off).	Podpisana pogodba; imenovana projektna organizacija; zapisnik začetnega sestanka; vzpostavljena projektna orodja in repozitoriji.
M+1,5	Potrditve analize in projektne priprave.	Poročilo o analizi vrzeli; usklajen popis zahtev; konceptualna tehnična zasnova; načrt testiranja in kakovosti; začetni register tveganj; posodobljen terminski plan.
M+6	Demonstracija rešitve in zaključek testiranja s strani izvajalca.	Zapisnik demonstracije; dobavljena verzija za formalna testiranja; poročilo o internem testiranju (unit/integracijsko/regresijsko); seznam odprtih napak in načrt odprave.
M+8	Zaključek uporabniškega in varnostnega testiranja v testnem okolju.	Zapisnik UAT/SAT; poročilo varnostnih testov; potrjena odprava kritičnih napak; odločitev o prehodu v pilotno okolje.
M+9	Zaključek testiranja migriranih podatkov v pilotnem okolju in potrditev izračunov.	Poročilo o migraciji in validaciji podatkov; primerjalni test izračunov; zapisnik o potrditvi izračunov.
M+10	Primopredaja, prehod v poprodukcijsko podporo in začetek redne uporabe; prehod v redno vzdrževanje.	Končni prevzemni zapisnik; predana dokumentacija in koda; operativni runbook; izvedena usposabljanja; aktivirana poprodukcijska podpora (hypercare) v obdobju 1 meseca in vzdrževalni režim/SLA.

Opomba: navedeni mejniki so okvirni in izraženi relativno glede na začetek pogodbe (M+X). Izvajalec mora v okviru faze 1 pripraviti in uskladiti podroben terminski plan s koledarskimi datumi, odvisnostmi in rezervami za testiranje ter odpravo napak.

7. Izhodna strategija

Izvajalec mora kot del ponudbe pripraviti celovito izhodno strategijo, usklajeno s predlagano arhitekturo rešitve in uporabljene tehnologije. Izhodna strategija mora zagotoviti, da v primeru prenehanja vzdrževanja in prehoda na drugega izvajalca naročnik obdrži vsa vlaganja v rešitev in mora naročniku kadarkoli omogočiti, da sam nadaljuje z razvojem (lahko s pomočjo drugega ponudnika). Izvajalec mora strategijo uskladiti z naročnikovimi smernicami za upravljanje s tveganjem dobavnih verig, ki jih podajamo v nadaljevanju.

Namen takšne strategije je zaščititi naročnika pred preveliko odvisnostjo od izvajalca (t.i. *vendor lock-in*) in zagotoviti nemoteno nadaljevanje uporabe ter vzdrževanja rešitve ob zaključku sodelovanja - regulatorni okvirji, kot je NIS2/ZInfV-1, izrecno poudarjajo nujnost načrtovanih izhodnih postopkov za kritične ICT storitve.

Tudi smernice dobrih praks (npr. standardi ISO/IEC 27036 za odnose z dobavitelji in ISO/IEC 12207 za življenjski cikel programske opreme) organizacijam svetujejo, da že v pogodbah s ponudniki opredelijo postopke v primeru prenehanja sodelovanja. V nadaljevanju predstavljamo ključne elemente celovite izhodne strategije, ki pokriva redne in izredne scenarije, različne tipe izvajalcev in tehnoloških rešitev, ključne obveznosti izvajalca ter pravno-tehnične vidike (skladno z ZJN-3, ZInfV-1/NIS2, GDPR in drugimi relevantnimi predpisi), pri čemer je poseben poudarek namenjen mehanizmu prenosa znanja in kontinuitete storitev ter ureditvi obveznosti pri prehodu na novega izvajalca.

Izbrani ponudnik bo moral pripravljene izhodni strategiji slediti skozi celoten življenjski cikel projekta slediti; te smernice pa vsebujejo ključne elemente politik in pravilnikov naročnika, vezanih na pripravo izhodnih strategij in jih bo naročnik uporabljal pri presoji ustreznosti pripravljene strategije v ponudbi.

Izhodna strategija, ki upošteva vse navedene smernice je pogoj za tehnično ustreznost ponudbe in bo sestavni del pogodbe; ponudba, ki ne pripravi skladne izhodne strategije je nedopustna.

Scenariji izhoda: redni in izredni

Redni izhod nastopi ob normalnem, načrtovanem zaključku pogodbenega razmerja - npr. po izteku pogodbe ali ob zaključku projekta. Pri rednem izhodu ima naročnik in izvajalec praviloma vnaprej določen prehodni rok in načrt aktivnosti za predajo rešitve. Že v končni ponudbi naj bosta določena časovni okvir in način primopredaje, da se ob zaključku zagotovi nemoten prevzem sistemov, kode in dokumentacije.

Izredni izhod se aktivira v nepredvidenih okoliščinah, kot so npr. insolventnost ali stečaj izvajalca, hude kršitve pogodbenih obveznosti, resni varnostni incidenti ali drugi razlogi za izredno odpoved pogodbe; za takšne primere mora strategija vključevati omilitvene ukrepe. Borzen zato skozi celoten življenjski cikel upravljanja pogodbenega razmerja upošteva tveganja na strani ponudnika (npr. njegov morebitni poslovni neuspeh ali poslabšanje kakovosti

storitev). Izhodna strategija zato predvideva takojšnje in kontinuirane ukrepe za zaščito naročnika - npr. preklic dostopov, redno vodenje izvorne kode pri naročniku, prehod na rezervnega izvajalca ali interno ekipo, ter načrte za vzpostavitev začasnih rešitev, če pride do nenadne prekinitve storitev.

Pomembno je razlikovati med postopki pri rednem in izrednem izhodu, je pa v obeh primerih cilj enak: omogočiti naročniku, da brez večjih motenj v poslovanju nadaljuje z uporabo, vzdrževanjem in razvojem programske opreme, bodisi samostojno bodisi z novim partnerjem.

Vrste izvajalcev in kombinacije tehnoloških rešitev

Izhodna strategija mora biti prilagojena organizacijski strukturi izvajalca ter tehnološki zasnovi rešitve.

Tehnološke rešitve

Lastni razvoj, prilagoditve obstoječih rešitev in odprta koda

Projekti se razlikujejo po tehnološki zasnovi: lahko gre za popolnoma prilagojen (lastni) razvoj, za prilagoditev obstoječe komercialne rešitve ali pa za integracijo odprtokodnih rešitev in knjižnic. Izhodna strategija mora pokriti vse relevantne scenarije, glede na pristop, ki ga je izbral ponudnik:

- Pri popolnoma namensko razviti programski opremi (»greenfield« razvoj) je ključna izročitev izvorne kode in dokumentacije, saj je celotna koda specifična za naročnika. Naročnik mora pridobiti materialne avtorske pravice in znanje za nadaljnji razvoj te kode.
- Pri prilagoditvi obstoječih rešitev (npr. nadgradnja obstoječega sistema ali uporaba zaprte komercialne platforme tretjega ponudnika) je treba zagotoviti, da ima naročnik ustrezno licenco za nadaljnjo uporabo in prilagajanje te platforme tudi po izhodu izvajalca, ter da ima obstoječa rešitev dobro definirano obdobje in politiko vzdrževanja, skladno z zahtevami ZInfV-1/NIS2, ter je prosto dostopna na trgu, kot samostojna rešitev. Če izvajalec vpelje npr. produkt tretjega ponudnika, mora zagotoviti, da bo naročnik lahko neposredno sklenil pogodbo s tem ponudnikom ali da dobi prenos licence na njega. Če ponudnik ponuja lastno rešitev (platformo), ali platformo, ki ni prosto dostopna na trgu, ali je ne razvija večji principal, mora naročniku zagotoviti izvirno kodo in licenco za lastno prilagajanje rešitve za svoje potrebe.
- Pri uporabi odprtokodnih komponent je prednost ta, da so načeloma prosto dostopne in jih lahko vzdržuje kdorkoli, vendar pa je treba paziti na licenčne pogoje odprtokodnih knjižnic, ki od naročnika ne smejo zahtevati objave izvorne kode rešitve.

Izvajalec mora zagotoviti evidenco vseh odprtokodnih komponent (t.i. *Software Bill of Materials*, SBOM) in slediti skupnosti, ki komponente razvija, glede posodobitev ali prenehanja vzdrževanja. Če določena odprtokodna komponenta doseže konec življenjske dobe (EOL) ali postane nevzdrževana, mora izvajalec pravočasno integrirati novejšo različico ali nadomestno komponento.

Kombinacije tehnoloških rešitev (npr. lastni razvoj, ki vključuje odprto kodo in komercialni moduli tretjih ponudnikov) zahtevajo posebno obravnavo - kot navajajo smernice *Linux Foundation*, se danes programski produkti pogosto gradijo v multi-source modelu: kombinacija lastne kode, odprtokodne kode in komercialnih komponent, zato je za uspešen izhod ključno, da ima naročnik pregled nad vsemi temi deli in ustrezne pravice za vsakega.

Izhodna strategija mora nasloviti vsakega od virov: za lastno razvite dele - prenos pravic intelektualne lastnine ali vsaj neomejeno licenco; za odprtokodne dele - skladnost z licencami in kopije kode; za komercialne dele - prenos licence ali zamenjavo z odprtimi alternativami ob izhodu.

Naročnik ponovno poudarja, da mora tudi po prenehanju pogodbe z izvajalcem imeti neokrnjeno možnost uporabe in nadaljnjega vzdrževanja vseh delov rešitve brez dodatnih stroškov za koriščenje materialnih avtorskih pravic (npr. dodatne licenčnine ob prenehanju, ipd.); glede na izbrano strategijo implementacije mora zato izvajalec za vsak del rešitve jasno opredeliti, kako bo to zahtevo naslovil.

Ključne obveznosti izvajalca za zagotovitev uspešnega izhoda

V pogodbo je vključen nabor obveznosti, ki bodo naročniku omogočile nemoten prevzem sistema v lastno upravljanje ali prenos k drugemu ponudniku. Ključna področja obveznosti so:

- (a) prenos izvirne kode in dokumentacije,
- (b) licenciranje za časovno in krajevno neomejeno lastno uporabo (vključno z nadaljnjim razvojem),
- (c) zagotavljanje pravic za interno zaprto uporabo (brez obveznosti objave kode navzven),
- (d) podpora in vzdrževanje (tudi odprava varnostnih ranljivosti) skozi dogovorjeno obdobje,
- (e) pregled nad življenjskim ciklom uporabljenih komponent (s politiko ukinitve/deprecacije).

Prenos izvirne kode in popolne dokumentacije

Izvajalec mora naročniku izročiti (in sproti, med razvojem, posodablјati) vso izvirno kodo razvite rešitve (in uporabljenih delov), skupaj s pripadajočo tehnično dokumentacijo, navodili

za namestitve, konfiguracijo in uporabo ter z vsemi drugimi artefakti, ki so potrebni za prevzem nadzora nad programsko opremo. Ta obveznost velja tako ob rednih mejnikih, kot ob izteku ali prekinitvi pogodbe (končna predaja celotnega repozitorija kode in dokumentacije). Pri tem mora ponudnik zagotoviti, da se zadnja različica izvirne kode skupaj z vso zgodovino sprememb v obliki Git v naročnikovo hrambo prenese najmanj vsakih 14 dni.

Edina izjema so na trgu prosto dostopne, redno vzdrževane rešitve, ki imajo jasno opredeljen življenjski cikel vzdrževanja in ustrezno podporo, ki ni vezana na izvajalca rešitve (primeri takšnih rešitev, ki jih naročnik že uporablja, so: Microsoft Windows, Microsoft SharePoint, MicroStrategy ipd.): za njih izvajalcu ni potrebno zagotoviti izvirne kode, mora pa skladno z že omenjenimi zahtevami zagotoviti ustrezne licence ali drug način prenosa pravic, ki naročniku omogočajo nadaljnjo uporabo in vzdrževanje rešitve, brez dodatnih stroškov ob izhodu.

Prav tako mora izvajalec predati vso dokumentacijo: tako tehnično dokumentacijo (arhitektura rešitve, podatkovni modeli, API specifikacije, opis komponent, konfiguracije, testni načrti) kot uporabniško dokumentacijo (navodila za uporabo, administracijo ipd.). Pomemben je tudi prenos dokumentacije o okolju (npr. infrastruktura, nastavitve strežnikov, gesla in dostopi, če jih vzdržuje izvajalec) - le s celovito in ažurno dokumentacijo bo lahko naročnik ali nov izvajalec sistem razumel in ga uspešno vzdrževal.

Licenca za časovno in krajevno neomejeno lastno uporabo, vzdrževanje in razvoj

Naročnik mora prek pogodbe pridobiti jasno opredeljene pravice intelektualne lastnine nad rezultati projekta - v praksi to pomeni, da je naročnik v pogodbi definiral neomejeno pravico uporabe rešitve z možnostjo samostojnega nadaljnjega razvoja. To lahko dosežemo bodisi s prenosom avtorske pravice na naročnika (kjer je to mogoče), ali pa s podelitvijo licence, ki je: trajna (časovno neomejena), geografsko neomejena, prenosljiva (vsaj na povezana podjetja oz. na novega vzdrževalca) in zajema pravico do nadaljnjega razvijanja.

Ključna je pravica, da sme naročnik programsko opremo spreminjati in prilagajati za svoje potrebe ter jo poganjati v svojih okoljih brez dodatnih licenčnih stroškov - tudi, če avtorska pravica morda ostane pri izvajalcu, mora licenca učinkovati podobno kot lastništvo - naročniku omogočati vse oblike lastne uporabe. To vključuje tudi pravico, da po potrebi najame tretjo osebo (npr. novega izvajalca) za vzdrževanje ali nadgradnje, ne da bi potreboval soglasje prvotnega izvajalca.

Pri določanju licenčnega režima je treba upoštevati tudi komponente, ki jih je morda zagotovil izvajalec, a niso njegove (ni nosilec avtorskih pravic): če je vključena komercialna komponenta tretje osebe (npr. licenčna knjižnica ali vgrajen modul), mora izvajalec poskrbeti, da naročnik dobi neposredno licenco te tretje osebe. Pri tem mora pri pripravi izhodne strategije izvajalec upoštevati tako komponente, ki so potrebne za delovanje rešitve, kot tiste, ki so potrebne za njen nemoten razvoj.

Za več informacij izvajalcem svetujemo, da preverijo Smernice za javno naročanje informacijskih rešitev (https://ejn.gov.si/dam/jcr:e4e8b815-bc00-41d9-b4cf-ac3aaea086aa/Smernice_JN_IT.pdf), ki jim naročnik pri svojem naročanju sledi.

Zagotavljanje pravic za zaprto uporabo (brez obveznosti objave kode)

Pri projektih, ki vključujejo odprtokodne komponente ali morebitne prispevke v odprto kodo, je za naročnika pomembno, da uporaba takšnih komponent ne sproži neželenih licenčnih obveznosti, kot je npr. zahteva po odprtju lastne izvirne kode. Nekatere močne copyleft licence (npr. GNU GPL ali še posebej AGPL in izpeljanke) lahko ob določenih načinih distribucije programske opreme zahtevajo, da se izvirna koda deli naprej.

Zato mora izvajalec zagotoviti, da v rešitvi ne bodo uporabljene odprtokodne komponente z licencami, ki imajo omejitve ali zahteve glede rabe ali distribucije izvirne kode, razen če za to dobi izrecno soglasje naročnika in so vzpostavljeni mehanizmi za izključitev tovrstnih obveznosti.

Izvajalec naj prednostno uporablja licence z nizkim tveganjem (t.i. permisivne licence, kot so MIT, BSD, Apache) namesto licenc z visokim tveganjem kot sta GPL ali AGPL.

Ne glede na izbor licenc mora izvajalec zagotoviti skladnost z odprtokodnimi licencami (*open-source compliance*). To pomeni, da mora:

- (1) naročniku predati seznam vseh odprtokodnih komponent in njihovih licenc,
- (2) priložiti vsa potrebna licenčna obvestila, izvirno kodo ali povezave do nje, kadar to licence zahtevajo,
- (3) zagotavljati, da uporaba komponent ne krši licenčnih pogojev.

Podpora, vzdrževanje in odpravljanje varnostnih ranljivosti

Ena ključnih obveznosti izvajalca je zagotavljanje podpore in vzdrževanja programske opreme vsaj do zaključka pogodbe oziroma v vnaprej dogovorjenem obdobju po izročitvi. To vključuje redno odpravljanje napak, prilagoditve na spremembe okolja in še posebej odzivanje na varnostne ranljivosti. V času trajanja pogodbe mora imeti naročnik zagotovilo, da bo izvajalec kritične napake in ranljivosti odpravil v dogovorjenem odzivnem času (SLA) **in v okviru pogodbenega pavšala.**

Izvajalec mora v svoji strategiji predvideti tudi situacijo, ko določena ranljivost izvira iz komponente, ki je zunaj nadzora izvajalca - na primer odprtokodna knjižnica ali platforma, ki jo ta uporablja, njen originalni vzdrževalec pa več ne izdaja popravkov (t.i. opuščena komponenta), ali proizvajalec tretje strani, ki ne podpira več stare verzije. Podobno velja tudi

v primerih zamenjave licenčnih pogojev odprtokodnih knjižnic iz dovoljene licence, na za naročnika nesprejemljivo licenco (npr. zamenjava licence iz MIT na GPL, ipd.).

Ker je izbira in odločitev o uporabi zunanjih komponent na strani izvajalca, se izvajalec zavezuje zagotoviti popravek ali zamenjavo za ranljivo / ne-vzdrževano komponento, četudi zanjo uradno ni več podpore in to v okviru rednega vzdrževanja in brez dodatnih stroškov za naročnika. To v praksi pomeni, da lahko izvajalec sam razvije varnostni popravek (npr. patch za odprtokodni projekt, ki ga uporablja) ali integrira novejšo alternativo / nadomesti komponento z lastnim razvojem. Naročnik ne sme ostati ranljiv zgolj zato, ker "principal" (izvorni avtor komponente) več ne zagotavlja popravkov - izvajalec mora to breme v celoti prevzeti kot del rednih vzdrževalnih obveznosti.

Izjema tega pravila so komponente iz naročnikovega tehnološkega portfelja, ki jih je izrecno opredelil v dokumentaciji in jih naročnik že uporablja - za njih ima naročnik zagotovljeno vzdrževanje in preverjeno dobavno verigo in za njih lahko samostojno zagotavlja varnostne popravke (npr. Microsoft .NET, Microsoft SQL, MicroStrategy, ipd.); izvajalec mora v okviru pogodbenega pavšala za te tehnologije predvideti zgolj morebitne posodobitve na svoji rešitvi zaradi nujnih varnostnih popravkov uporabljenih komponent, pri čemer so v preventivno vzdrževanje vključeni zgolj popravki zaradi varnostnih posodobitev (security update), ne pa tudi funkcionalnih nadgradenj uporabljene opreme iz tehnološkega portfelja naročnika.

Del vzdrževalnih obveznosti je tudi dogovorjeno prehodno vzdrževanje po prenehanju pogodbe, ki naročniku omogoča, da od izvajalca še 90 dni po prenehanju pogodbe zahteva izvajanje določenih storitev, vezanih na prehod izvajanja na naročnika ali novega izvajalca.

Dokumentiran življenjski cikel komponent in politika ukinitve (deprecation)

Izvajalec lahko predvidi programske rešitve, ki so sestavljene iz več komponent: lastne kode različnih modulov, knjižnic, okvirov (frameworkov), podatkovnih baz, operacijskih sistemov itd. Vsaka od teh komponent ima svoj življenjski cikel - nove verzije, popravke in tipično tudi konec podpore. Da se naročnik izogne situaciji, ko bi leto ali dve po prevzemu sistema ugotovil, da ta temelji na zastareli tehnologiji brez podpore (kar otežuje vzdrževanje in povečuje varnostna tveganja), mora izvajalec predstaviti strategijo upravljanja življenjskega cikla komponent.

To pomeni, da izvajalec že ob začetku identificira ključne tehnologije v rešitvi (npr. programski jezik in verzijo, baze podatkov, strežniške komponente, odprtokodne knjižnice itd.) in za vsako navede trenutno verzijo ter predvideno dobo uporabnosti. Obvezati se mora, da bo spremljal načrte ukinitve (deprecation) ali prenehanja podpore za te komponente ves čas trajanja pogodbe. Izvajalec mora kot del izhodne strategije definirati tudi politiko poročanja naročniku - na primer letno poročati o stanju komponent in predlagati nadgradnje, če katera doseže EOL.

Če pride do ukinitve določene komponente, mora izvajalec zagotoviti pravočasno migracijo na drugo ustrezno komponento, pri čemer stroške in vpliv na naročnika v času trajanja pogodbe nosi izvajalec. Na ta način se sistem stalno posodablja in ostaja v okviru podprtih tehnologij,

izvajalec pa določenih tveganj, ki izhajajo iz prevzema razvoja te rešitve ne more preprosto prenesti na naročnika in se tako znebiti odgovornosti.

Podobno kot v opisu zahtev glede vzdrževanja, velja tudi v primeru ukinitve komponent iz naročnikovega portfelja tehnologij (tehnologije, ki so navedene v specifikaciji in jih zagotavlja in vzdržuje naročnik): v primeru, da je izvajalec izbral takšno tehnologijo, dela vezana na nadomestitev te komponente zaradi njene ukinitve niso del rednega preventivnega vzdrževanja in niso vključene v pavšal.

Izvajalec mora v okviru analize projekta pripraviti dokument "*Strategija življenjskega cikla*", ki vsebuje seznam vseh ključnih komponent, njihovih verzij, virov (lastna koda, odprta koda ali komercialna komponenta), licenco, trenutni status podpore in predviden datum do kdaj bo komponenta posodobljena. Vključuje tudi politiko zamenjav: npr. "Če knjižnica X ne bo več vzdrževana, jo bomo nadomestili z Y, ki ima podobno funkcionalnost." Ta dokument se med projektom redno posodablja: naročniku to zagotavlja pregled in vpliv na tehnično zdravje rešitve, kar je ključno za dolgoročno vzdrževanje po izhodu izvajalca.

Mehanizmi prenosa znanja in kontinuitete storitev

Poleg formalnih pogodbenih določil je ključno, da se vzpostavijo tudi praktični mehanizmi za prenos znanja med izvajalcem in naročnikom (oziroma novim izvajalcem) - dokumentacija sama po sebi ni vedno dovolj; potrebno je aktivno sodelovanje in usposabljanje naročnikovih ekip. Dobre prakse za zagotovitev kontinuitete vključujejo:

- Sodelovanje naročnikovega kadra v projektu: če je mogoče, naj izvajalec predvidi sodelovanje strokovnjakov naročnika v projektnih aktivnostih (npr. kot del razširjene ekipe, pri testiranjih ali spremljanju razvoja). Tako naročnik sproti pridobiva vpogled v rešitev in tehnologije, ob odhodu izvajalca pa bodo ti notranji strokovnjaki dragocen vir znanja. Projekt mora biti zasnovan tako, da je v vsak profil vključen tudi naročnikov kader (npr. arhitekt, razvijalec, infrastrukturni strokovnjak).
- Redne delavnice in treningi: izvajalec naj periodično izvaja tehnične delavnice za naročnikov IT oddelek - npr. ob zaključku pomembne faze predstavi arhitekturo in implementacijo modula, odgovori na vprašanja in dokumentira morebitne prilagoditve. Na koncu projekta naj se izvede celovit *knowledge transfer* sestanek ali serija delavnic, kjer izvajalec prenese znanje o vseh vidikih sistema (poslovna logika, konfiguracija, vzdrževanje, postopki odpravljanja napak). Izvajalec mora stroške za te aktivnosti predvideti kot del projektnih stroškov in program delavnic v ponudbi tudi podrobno opredeliti.
- Dostop do razvojnih orodij in okolij: naročnik zahteva dostop do razvojnega in testnega okolja, repozitorija kode, sistema za sledenje hroščev (bug tracker) in dokumentacijskih portalov (wiki ipd.), ki jih izvajalec uporablja; hkrati naročnik zagotavlja lasten repozitorij kode in dokumentacije, ki ju mora izvajalec redno posodabljati. S tem ima

vpogled v sprotni potek dela in se lahko lažje vključi. Ob koncu projekta se ti sistemi prenesejo (njihova vsebina) na naročnika.

- Preizkus izhodnega načrta: kot del zagotavljanja kontinuitete je priporočljivo, da naročnik in izvajalec skupaj preizkusita določene elemente izhodne strategije že med trajanjem pogodbe - izvajalec naj v izhodni strategiji to smiselno predvidi glede na izbran pristop.

Obveznosti ob prehodu na novega izvajalca

Ko pride do zamenjave izvajalca (bodisi redno ob poteku pogodbe, bodisi izredno), morajo biti jasno določene obveznosti odhajajočega izvajalca, kot vloge naročnika.

Izvajalec naj v svoji izhodni strategiji predvidi, kako bo zagotovil sodelovanje v prehodnem obdobju; to vključuje: pravočasno izročitev vse kode, dokumentacije in orodij; pojasnila in odgovarjanje na vprašanja nove ekipe; prisotnost na skupnih sestankih, kjer se razrešujejo odprta tehnična vprašanja. Odhajajoči izvajalec naj pripravi poročilo o stanju sistema ob predaji - kaj vse teče, verzije, znane odprte napake ali tehnični dolg, posebnosti konfiguracije itd. Pomembno je določiti, kako dolgo bo odhajajoči izvajalec nudil pomoč.

Pri tem dela, ki so vezana na predajo novemu izvajalcu in presegajo predvidene redne aktivnosti iz specifikacije (primeri predvidenih rednih aktivnosti: dokumentiranje kode in postopkov, priprava navodil za vzpostavitev), štejejo kot dodatna dela in se obračunajo po dogovorjeni postavki.

Obvezna določila pripravljene strategije

Izvajalec mora izhodno strategijo prilagoditi glede na izbrano rešitev, pri čemer mora upoštevati navodila, navedena v tem poglavju. Ne glede na izbrano rešitev, mora izhodna strategija na vsak način jasno zagotoviti:

- izvajalec se zavezuje, da bo po zaključku razvoja programske kode zagotavljal podporo in vzdrževanje za čas vzdrževanja po tej pogodbi. Vzdrževanje vključuje odpravo napak, zagotavljanje posodobitev, prilagoditve ter pomoč pri težavah, ki nastanejo pri uporabi sistema. Varnostne posodobitve in odprava napak morajo biti vključeni v pogodbeni pavšal za vzdrževanje in jih izvajalec ne sme obračunavati posebej.
- V primeru odstopa od pogodbe, izvajalec zagotovi pomoč pri prehodu in zagotovi podporo za prenos vseh potrebnih podatkov, dokumentacije in znanja, da bo naročnik lahko samostojno upravljal sistem; izvajalec mora že od začetka uporabe sistema zagotavljati vse potrebne avtorske (in druge) pravice, da ima naročnik kadarkoli možnost sam vzdrževati rešitev ali za njeno vzdrževanje najeti tretjo osebo.

- Po zaključku pogodbenega razmerja, izvajalec v roku 30 dni zagotovi prenos vseh podatkov, povezanih s sistemom, naročniku v obliki, ki je primerna za nadaljnjo obdelavo in uporabo. To vključuje vse baze podatkov, dokumentacijo, vire kode in vse konfiguracije za vsa okolja (razvojno, testno, produkcijsko).
- Vso dokumentarno gradivo v fizični ali elektronski obliki, ki nastane med delom izvajalca za naročnika po tej pogodbi, postane last naročnika.