Příloha K.1 Smlouvy
Kvalitativní vlastnosti Projektu a Služeb

Nový webový portál Karlovarského kraje

1. KONVENCE TOHOTO DOKUMENTU

1.1. Konvence tohoto dokumentu

1.1.1. Pro potřeby této přílohy jsou slovem web označeny všechny webové projekty a podprojekty, které jsou veřejně přístupné běžným uživatelům (ať už registrovaným nebo bez registrace).

1.1.2. Slovem administrace jsou pak označeny všechny editační, administrační rozhraní a nástroje, které pro Zákazníka vytvořil nebo vytváří Dodavatel.

1.1.3. Slovem systém se označují weby i administrace.

1.1.4. Všechny body požadavků jsou uvedeny v přítomném či minulém čase a pokud možno bez použití kondicionálů proto, aby každý požadavek šlo vyhodnotit jako splněný či nesplněný jednoduchou odpovědí ano / ne podle jeho aktuálního reálného stavu v době akceptace. Použití minulého času v tomto dokumentu neznamená automatické potvrzení Zákazníka o splnění tohoto bodu. Splnění či nesplnění požadavku je vždy předmětem akceptačního řízení.

1.1.5. Pokud z kontextu nevyplývá jinak, slova a slovní spojení v jednotném čísle zahrnují i množné číslo a naopak.

2. ORGANIZAČNÍ A PRÁVNÍ POŽADAVKY

2.1. Organizační požadavky

2.1.1. Všechny komplexní požadavky na systém vychází z provedených detailních analýz požadavků a jsou zpracovány v písemné podobě kterou schvaluje Zákazník.

2.2. Licence

2.2.1. Licence je upravena ve Smlouvě. Zákazník ke všem Výstupům, u kterých je to možné vzhledem k jejich charakteru, obdrží zdrojové soubory včetně dokumentace a komentářů a v případě zdrojových kódů i jejich kompletní historii.

2.2.2. Počet administrátorů (editorů) ani uživatelů (zákazníků) není licenčně omezen ani samostatně zpoplatněn.

2.2.3. Veškeré použité součásti nejsou zatíženy licenčními ani jinými podobnými periodickými poplatky.

2.3. Právní a další předpisy

2.3.1. Systém je významným informačním systémem veřejné správy ve smyslu zák. č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů, protože zajišťuje vedení úřední desky způsobem umožňujícím dálkový přístup.

2.3.2. Dodavatel při vytváření systému a poskytování služeb dodržuje právní předpisy a interní předpisy Zákazníka. Zákazník upozorňuje zejména na:

a. Nařízení (EU) 2016/679 (GDPR).

b. Směrnice (EU) 2002/58/ES (Nařízení o soukromí a elektronických komunikacích) a Nařízení, které ji nahrazuje (ePrivacy).

c. Zákon č. 480/2004, Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů, (zejména pak §7).

d. Zákon č. 99/2019 Sb. o přístupnosti internetových stránek a mobilních aplikací, ve znění pozdějších předpisů.

e. Zákon 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

f. Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

g. Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, v souvislosti s dálkovým přístupem na úřední desku.

h. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.

i. Požadavky ze směrnice NIS – týká se e-služeb (viz http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN).

j. Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů, a související změnový zákon č. 298/2016 Sb. (pro e-služby s autentizací).

k. Zákonem č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů.

l. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

m. Nutný soulad s interními bezpečnostními instrukcemi a politikami Zákazníka (příloha Zadání P.1.2).

3. TECHNICKÉ POŽADAVKY

3.1. Domény a DNS

3.1.1. Všechny nové registrace a prodloužení domén jsou zpracovávány Zákazníkem a na jeho odpovědnost.

3.1.2. DNS je ve správě Zákazníka a všechny změny podléhají schválení Zákazníkem, pokud se nejedná o předem dohodnutý automatický proces (např. failover). Dodavatel musí přizpůsobit vlastnosti systému a nastavit procesy tak, aby toto nezpůsobovalo prodlevy, výpadky či organizační problémy.

3.2. E-mail

3.2.1. Všechny e-maily, které jsou posílány jménem (tj. z domén) Zákazníka jsou zasílány přes Zákazníkem předem schválené SMTP servery či služby, pro které jsou korektně nastavené DNS (SPF, DKIM atp.) záznamy.

3.2.2. E-maily odesílané z webu nejsou posílané jménem (tj. z domény) návštěvníka/uživatele/partnera, pokud není zajištěna doručitelnost (SPF, DKIM, DMARC) těchto e-mailů.

3.2.3. E-mail obsahuje jméno odesílatele a subject v souladu s aktuálními best practices - např. délka, (ne)použití emojis, interpunkce, verzálek.

3.2.4. U HTML e-mailů existuje i TXT verze.

3.2.5. E-mail je korektně zobrazen minimálně 90 % příjemcům a v nejpoužívanějších mailových klientech (Gmail, Seznam, Yahoo, Outlook, Apple mail). Systém nemusí odlišovat "dark-mode" režim pro zobrazení e-mailů.

3.3. Internacionalizace a lokalizace

3.3.1. Celé řešení je realizováno s použitím kódování znaků UTF-8.

3.3.2. Systém umožňuje implementaci webu pro všechny evropské země a oficiální jazyky EU (abeceda, řazení, směr psaní, formáty čísel /např. telefon, PSČ, formátování čísel atp./, měna, fyzikální jednotky, formáty papíru, zvyklosti zápisu data a času včetně používání různých kalendářů a časových pásem).

3.3.3. Weby jsou validní podle https://validator.w3.org/i18n-checker/.

3.3.4. Používá se HTML atribut lang.

3.4. Kompatibilita a interoperabilita

3.4.1. Jsou využity technologie standardizované organizacemi jako např. W3C, Ecma International, IEEE atp., které podporují přístupnost a kompatibilitu s různými výstupními zařízeními, tedy typicky validní HTML, CSS, JavaScript atd.

3.4.2. HTTP metody jsou používány korektně s ohledem na jejich idempotence / safety.

3.4.3. Web se zobrazuje korektně i se zapnutými nejběžnějšími adblockery.

3.4.4. Dodavatel určí a zdokumentuje ve spolupráci se Zákazníkem relevantní šířky viewportu, a pro tyto šířky je zobrazení webu testováno.

3.4.5. Systém plnohodnotně podporuje Referenční platformy, které jsou:

a. prohlížeče Google Chrome a Safari v posledních dvou hlavních verzích, nainstalované na počítači s operačním systémem macOS verze 10.15 a vyšší.

b. prohlížeče Microsoft Edge, Google Chrome a Mozilla Firefox v posledních dvou hlavních verzích, nainstalované na počítači s operačním systémem Microsoft Windows verze 10 a vyšší.

c. prohlížeč Safari, instalovaný na mobilním zařízení s operačním systémem Apple iOS v předposlední hlavní verzi a novější.

d. prohlížeč Google Chrome v posledních dvou hlavních verzích, instalovaný na mobilním zařízení s operačním systémem Android a Apple iOS.

3.4.6. Mimo referenční platformy se využívá přístupu pozvolné degradace (graceful degradation) pro zajištění co nejširší relevantní kompatibility.

3.5. Frontend / HTML, CSS, Obrázky, Video

3.5.1. Web má vhodné ikony a favicon pro všechny relevantní platformy.

3.5.2. Web neobsahuje odkazy vedoucí na neexistující adresy (HTTP 404).

3.5.3. Web nenačítá zdroje (CSS, JS, obrázky, …) z neexistujících adres (HTTP 404).

3.5.4. Weby mají nastavený viewport stránky

3.5.5. Používají se správné vstupní prvky (HTML5 input type) podle druhu zadávaných dat.

3.5.6. Používají se sémantické elementy HTML5 (header, section, footer, main …).

3.5.7. Všechny hlavní šablony jsou testovány W3C validátorem pro identifikaci možných problémů.

3.5.8. V konzoli prohlížeče nejsou zalogovány žádné chyby ani ladící hlášení.

3.5.9. Při načítání webu nedochází k efektům FOIT (flash of invisible text).

3.5.10. Weby používají responzivní design. Breakpointy jsou nastaveny podle analýzy zařízení návštěvníků. Web se přizpůsobuje vlastnostem a rozměrům výstupního zařízení z hlediska velikosti písma, rozměrů klikacích/dotykových prvků. U mobilních telefonů a tabletů proběhlo přizpůsobení dotykovému ovládání (minimální ergonomické rozměry dotykových prvků, nezávislost na hover stavech).

3.5.11. Všechna ID na stránce jsou unikátní.

3.5.12. Videa jsou zajištěna skrze globální CDN řešení (přípustné i YouTube či Vimeo).

3.5.13. Obrázky se poskytují v alternativách dle podpory UA (nejlépe pomocí picture srcset, popř. dynamickou volbou mimetype dle UA). Alternativami jsou myšleny zejména relevantní případy vlastních obrázků:

a. vhodné rozměry obrázku podle výstupního zařízení (malé, velké)

b. vhodné formáty obrázku s přihlédnutím zejména na datovou velikost a charakter obrazové informace (preferovány moderní formáty SVG, WebP, JPEG 2000, JPEG XR, AVIF atp.).

3.5.14. Stránky, které dává na základě analýzy smysl tisknout, jsou upraveny pro tiskový výstup pomocí tiskových stylů. Tiskové výstupy jsou optimalizovány tak, aby spořily spotřební materiál uživatele (papír, toner).

3.6. Optimalizace pro vyhledávače

3.6.1. Není zakázaná indexace veřejného a publikovaného obsahu vyhledávači, pokud toto nevyplývá z explicitního funkčního požadavku.

3.6.2. Je nasazen korektní robots.txt.

3.6.3. Pro weby existuje relevantní, validní a aktuální Sitemap v XML formátu podle https://www.sitemaps.org/. V případě většího rozsahu (limit 50.000 záznamů nebo 50MB nekomprimovaně) je Sitemap rozdělena do více souborů uvedených v Sitemap index souboru. Může být použita gzip komprese. Sitemap je korektně odkázána v robots.txt.

3.6.4. Sitemaps jsou uvedeny v robots.txt

3.6.5. Systém robotům neblokuje přístup ani neposkytuje rozdílný obsah. Výjimku tvoří roboti, v případě že systém extrémně přetěžují (zejména známé botnety z Číny, Ruska, ...). Na tyto roboty je možné aplikovat přísný rate limiting.

3.6.6. Stejný obsah webů není duplicitně přístupný na více URL a na jednom URL není přístupné více stránek. Za různá URL se považují i URL lišící se jen počtem či hodnotami parametrů ("query").

3.6.7. URL webů nemá nadbytečné parametry nebo obsah v částech URL "query", či "path" a je co nejkratší (při zachování čitelnosti a dodržení SEO zadání či potřeb).

3.6.8. V částech "path" a "fragment" a názvech a hodnotách části "query" URL webů se používají jen písmena anglické abecedy, číslice, pomlčky (minus), tečky a lomítka.

3.6.9. Title a description stránek webu jsou automaticky generována z nadpisů či obsahu stránky, každá stránka má unikátní title. Je možné definovat vlastní title a description.

3.6.10. Hlavní obsah, položky navigace webů, hledání, kontakty, kategorie a produkty jsou dostupné bez JavaScriptu.

3.6.11. Na každé veřejné stránce jsou implementovány náhledy pro sociální sítě. Open Graph a Twitter Cards minimálně v rozsahu reprezentativního obrázku podle obsahu stránky.

3.6.12. Nad rámec základního HTML obsahuje zdrojový kód stránek i validní sémantické značkování vybraných objektů (události, místa, osoby apod.) podle specifikace Schema.org JSON-LD.

3.6.13. Jsou použity validní Google rich snippets pro všechna relevantní data, která Google podporuje (zejména Article, Breadcrumb, Review, Event, FAQ, How-to, Job Posting, Local Business Listing, Logo, Product, Q&A, Video).

3.6.14. Obsah, která má být indexovatelný je dostupný bez JavaScriptu.

3.7. Přístupnost

3.7.1. Všechny obrázky mají alternativní popis.

3.7.2. Web je ovladatelný pomocí klávesnice.

3.7.3. U webů jsou respektována Web Content Accessibility Guidelines 2.1 minimálně v úrovni shody AA.

3.7.4. Používá se značkování WAI-ARIA v souladu s https://www.w3.org/TR/wai-aria-practices/.

3.7.5. Všechny formulářové prvky na webech mají label nebo aria-label.

3.8. Rychlost

3.8.1. Není použitý "viewstate" ani podobný mechanismus komplikující cachování a zpomalující interakce s webem.

3.8.2. CSS a JavaScript soubory jsou minifikované.

3.8.3. Používá se brotli, popř. gzip komprese a současně ochrana proti BREACH zranitelnosti u přenosu osobních či citlivých dat.

3.8.4. Obrázky jsou optimalizované, včetně uživatelsky nahrávaných.

3.8.5. JavaScript se načítá v maximální možné míře pomocí async nebo defer či jinou metodou zajišťující neblokující vykreslování stránky.

3.8.6. V relevantních případech (dlouhé výpisy) se používá lazy loading obrázků.

3.8.7. Používají se jen nejnutnější cookies, session cookie se vytváří až je reálně potřeba (pro umožnění lepšího cachování).

3.8.8. Používá se maximálně 10 cookies, každá o max. velikosti 4 kB.

3.8.9. Používá se dns-prefetch.

3.8.10. Assety (statický obsah) mají velmi dlouhou dobu uchovávání v cache (max-age či expires). Invalidace se provádí změnou názvu assetu.

3.8.11. Je použit protokol HTTP/2 na přístup ke všem zdrojům; výjimkou jsou externí služby, kde to dodavatel není schopen ovlivnit.

3.9. Zabezpečení

3.9.1. Systém netrpí základními zranitelnostmi, zejména

- Aktuální OWASP Top 10
- Obcházení autorizace - např. přístup k datům jiných zákazníků/uživatelů nebo funkcím správce z běžného účtu
- Nezabezpečené session ID - např. token, který lze uhodnout; token uložený na nezabezpečeném místě atp.

- Injections - SQLi, NoSQLi, XXE, OS command injection, ...
- Cross-site scripting (XSS) - např. volání nezabezpečených funkcí JavaScriptu, provádění nezabezpečených manipulací s DOM, výpis uživatelského vstupu do HTML bez escapování.
- Cross-site request forgery (CSRF) - např. zpracování požadavků s hlavičkou Origin z jiné domény.
- Použití frontend i backend knihoven se známými zranitelnostmi
- Další zranitelnosti, které je možno detekovat běžnými automatizovanými nástroji

3.9.2. Nejsou veřejně přístupné interní a vývojové soubory a adresáře jako např. .git repozitář, konfigurační soubory pro vývoj, sestavení nebo provoz, source maps atp.

3.9.3. Jako zdroj aktuálních best practices je považován https://cheatsheetseries.owasp.org

3.9.4. Neexistují společné přístupové účty, každý pracovník Dodavatele i Zákazníka má samostatný přístup vedený na jeho jméno.

3.9.5. Uživatelé administrací mají k dispozici možnost aktivovat MFA (multi factor authentication, vícefaktorové ověřování). Pro role určené Objednatelem je použití MFA povinné.

3.9.6. Přístup k citlivým datům (osobní a přístupové údaje) je omezen výhradně na pracovníky s oprávněnou potřebou.

3.9.7. Oprávněná potřeba přístupu k citlivým datům je pravidelně kontrolována. Nadbytečné účty či přístupová oprávnění pracovníků bez oprávněné potřeby jsou bez zbytečného prodlení rušeny.

3.9.8. Je zajištěno, že neprodukční prostředí neobsahují produkční citlivá data. Dodavatel nekopíruje či nepřesouvá citlivá data z produkčního prostředí Zákazníka, pokud to Zákazník výslovně neschválil.

3.9.9. V případech, kdy systém zajišťuje autentizaci uživatelů, tak práce s hesly respektuje:

a. minimální délka hesla je 8 znaků
b. maximální délka hesla není omezena na méně než 64 znaků
c. nejsou omezeny povolené znaky, které lze použít
d. nepoužívají se tajné otázky jako jediný požadavek na obnovení hesla
e. při změně hesla se vyžaduje aktuální heslo a e-mailové ověření změny
f. nově vytvořená hesla jsou
    - ověřována podle seznamů běžných hesel

- algoritmicky kontrolována, že neobsahují opakování typu aaaa nebo sekvence typu 1234
- algoritmicky kontrolána, že v heslu není část e-mailu nebo jména uživatele či brandu, používaných značek Zákazníka

g. nově vytvořená hesla jsou ověřována podle databází uniklých hesel

h. hesla jsou ukládána v hashovaném a salted formátu za použití paměťově nebo výpočetně náročné jednosměrné hashovací funkce

i. při detekci útoků pomocí hrubé síly je vynuceno vhodné uzamčení / ochrana proti přístupu k účtu

3.9.10. Ve Version Control System (VCS) nejsou uloženy žádná privátní hesla, certifikáty, klíče, přístupové údaje atp. (secrets). Výjimku tvoří secrets, které jsou společně s ostatními konfiguračními parametry uloženy v samostatném repozitáři a šifrovány bezpečným způsobem.

3.9.11. Je nasazen soubor security.txt podle posledního Internet-Draft nebo RFC.

3.9.12. V případě, že použitá součást obsahuje bezpečnostní chybu střední a větší závažnosti relevantní k systému, je součást aktualizována nejpozději do 30 kalendářních dnů, pokud je splněno:

a. Chyba má přidělený CVE identifikátor a současně

b. Existuje opravná verze či workaround od Dodavatele či autora této součásti

c. Nedošlo k písemné dohodě o tom, že se chyba nebude řešit

3.9.13. Externí zdroje se nenačítají z protocol-relative URL.

3.9.14. Všechny HTTPS URL obsahují Strict Transport Security hlavičku.

3.9.15. Všechny cookie mají nastavený příznak Secure.

3.9.16. Session cookie mají nastavené příznaky HttpOnly a SameSite.

3.9.17. Významné akce, zejména v administrací, obsahují CSRF tokeny.

3.9.18. Používají se bezpečnostní hlavičky X-Frame-Options, X-Content-Type-Options, Referrer-Policy a Permissions-Policy.

3.9.19. Stránky při přístupu přes protokol HTTP korektně (tj. se zachováním FQDN) přesměrovávají na stejné URL s protokolem HTTPS.

3.9.20. Obsah a funkce jsou dostupné pouze pomocí protokolu HTTPS, přístup pomocí HTTP protokolu je umožněn pouze pro přesměrování na zabezpečenou variantu příslušného zdroje.

3.9.21. Všechny zdroje vkládané z jiných serverů, včetně iframes, jsou vloženy výhradně za použití protokolu HTTPS.

3.9.22. Je nastaven CAA záznam v DNS.

3.9.23. Je použit serverový certifikát schválený Zákazníkem. Jeho nasazování je automatizováno a platnost automaticky monitorována. Není použit certifikát s platností delší než 12 měsíců, klíč certifikátu se rotuje minimálně jednou ročně.

3.9.24. Není použito Public Key Pinning.

3.9.25. V URL není nikdy osobní údaj.

3.9.26. Na stránkách obsahujících osobní údaje je minimalizováno použití knihoven z "public CDN" - např. Google Hosted Libraries, BootstrapCDN atp. V těchto případech je vždy použito SRI (Subresource Integrity).

3.9.27. V systému jsou implementovány všechny relevantní funkcionality, které vyžaduje GDPR s ohledem na zpracovávané osobní údaje. Výjimku tvoří operace, které manuálně provede Dodavatel v rámci poskytování Podpory.

3.9.28. Inline JavaScript (script type="text/javascript") je povolen pouze s nonce atributem, který se mění pro každý Request. Inline application/json je povolený i bez nonce.

3.9.29. Je veden záznam o servisních zásazích na Infrastruktuře s přesnými záznamy času, pracovníka a provedené operace.

3.9.30. Systém obsahuje opatření pro skokový nárůst Návštěvníků webových stránek či hackerské útoky.

3.10. Zakázané technologie

3.10.1. Není používána klientská technologie Adobe Flash, Microsoft Silverlight, Oracle Java ani podobná, vyžadující binární pluginy v prohlížeči uživatele.

3.11. Chybové stavy, chybové stránky

3.11.1. Požadavek na neexistující obsah vrací stavový kód HTTP 404. Chyba backend serveru vrací stavový kód HTTP 50x, údržba stavový kód HTTP 503 a při aplikaci rate limitingu je klientovi vrácen stavový kód HTTP 429.

3.11.2. Existují lokalizované error pages (400, 401, 403, 404, 503 /maintenance/, ostatní 4xx, 5xx); všechny tyto stránky jsou "custom", jejich obsah se liší od standardních výchozích stránek webserveru.

3.12. Nasazování nových verzi

3.12.1. Při spouštění nového webu, který nahrazuje web stávající, postupoval Dodavatel tak, aby byl výpadek provozu během přechodu minimální, pokud možno nulový. Tj. pokusil se např. zajistit provoz přes proxy a zajistil si dopředu vhodný HTTPS certifikát. V žádném případě nedošlo k smazání libovolných dat, logů či nastavení původního webu.

3.12.2. Při spouštění nového webu, který nahrazuje web stávající, postupoval dodavatel tak, že se zvýšenou pozorností monitoroval a vyhodnocoval po dobu minimálně 10 dnů v souborech protokolu chyby 404. V případech, kdy toto URL mělo být funkční, zajistil jeho zprovoznění, či přesměrování v nejkratší možné lhůtě.

3.12.3. Při spouštění libovolného nového webu, který nahrazuje web stávající a současně je indexovaný vyhledávači, vypracoval dodavatel analýzu mapující URL všech stránek původního (stávajícího) webu na nový web a v okamžiku spuštění nového webu zajistil trvalé přesměrování starých URL na nové.

3.12.4. Součástí procesu vývoje a deploymentu je verzování databázových schémat a nastavení pro migraci dat nebo zajištění stejného či lepšího efektu, který tento požadavek zajišťuje.

3.12.5. Existuje více prostředí (minimálně vývojové, qa a produkční). Vývojovým prostředím je myšleno typicky lokální vývojové prostředí jednotlivého vývojáře či vnitrofiremní vývojové prostředí dodavatele. QA (Quality Assurance) prostředí je zpřístupněno Zákazníkovi pro testování funkčnosti a jedná se o prostředí technologicky velmi blízké produkčnímu prostředí (s menšími nároky na výkon a distribuovanost aplikace, pokud toto není předmětem testování). Produkčním prostředím je míněno prostředí veřejně přístupné návštěvníkům a administrátorům webů.

3.12.6. Jediné prostředí, které je veřejně přístupné, je produkční prostředí.

3.12.7. Pro vývoj a deployment jsou použity techniky a nástroje, které umožní automatizované nasazování a testování nových verzí aplikace. Popis nasazování je součástí dokumentace. Součástí deploymentu je automatizace přinejmenším těchto operací nebo zajištění stejného či lepšího efektu, který tyto operace poskytují:

a. build aplikace (včetně generování CSS a JS skriptů apod.),

b. přenos na cílové prostředí a kontrola závislostí,

c. přepnutí aplikace do maintenance modu (pokud je nutné),

d. migrace DB,

e. výměna aplikačního kódu,

f. vypnutí maintenance modu (pokud je nutné).

3.12.8. Postup nasazování na libovolné běhové prostředí je stejný pro všechna prostředí s výjimkou vývojového prostředí a je plně automatizován.

3.13. Praktiky a metodiky

3.13.1. Jsou vybrány a definovány vhodné standardy pro zajištění čistoty zdrojového kódu (coding standards). Popis standardů je součástí dokumentace zdrojového kódu.

3.13.2. Zdrojové kódy jsou verzovány pomocí DCVS/CVS nástroje a uloženy v repozitářích. Zákazník má stálý read-only přístup ke všem těmto repozitářům. Popis verzovacího workflow je součástí dokumentace.

3.13.3. Změny zdrojového kódu jsou do repozitářů promítány nejméně 1x týdně.

3.13.4. Funkce, které je možné a vhodné (nejen technicky, ale zejména z business logiky) realizovat asynchronně, jsou takto řešeny (např. rozesílání e-mailů).

3.13.5. Je použit přístup "Secure by design". Jsou použity frameworky, šablonovací jazyky nebo knihovny, které systémově řeší nedostatky implementace escapováním výstupů a sanitizací vstupů (např. ORM pro pro přístup k databázi, UI frameworky pro vykreslování DOM).

3.13.6. Dodavatel postupuje tak, aby nevznikal zbytečný technologický dluh. Technologickým dluhem je myšlen zejména:

a. důsledek postupů, které v zájmu krátkodobého zvýšení produktivity způsobí vznik provizorních řešení, která přinesou zvýšené náklady na vznik finálního řešení nebo jeho další rozvoj a údržbu;

b. důsledek nečinnosti, kdy se zastaráváním použitého řešení zvyšuje nákladnost aktualizace či provozu systému nebo kdy zastaralé řešení bude obsahovat bezpečnostně zranitelné součásti.

3.13.7. V případech, kde se vyplatí vědomě technologický dluh vytvořit a kde k takovému postupu Zákazník vyjádří souhlas není nutné dodržovat předchozí bod. Dodavatel upozornil Zákazníka na všechny případy, kdy identifikoval, že se vyplatí vytvořit technologický dluh.

3.14. Automatizace

3.14.1. Vývojový proces zahrnuje nástroje a postupy, které zajistí automatizovanou kontrolu dodržování coding standards (linter), pre/post procesory a compilery CSS či JS, buildovací a balíčkovací nástroje.

3.14.2. Všechny konfigurační soubory specifické pro aplikaci (například nastavení webového serveru, nastavení dalších komponent jako třeba Redis, MongoDB, Varnish cache apod.) jsou ukládány a verzovány v Git repozitáři, ke kterému má Zákazník read-only přístup. Tyto soubory se automaticky používají pro konfiguraci serverových součástí; u serverových součástí, kde toto

není možné nebo by bylo neadekvátně nákladné je toto nahrazeno dokumentací k ručnímu nastavení dané součásti (např. AWS CloudFront).

3.15. Externí služby

3.15.1. Všechny externí služby, které má Dodavatel záměr použít (včetně služeb jako Google Analytics, Google Tag Manager, Google Search Console, jiné cloudové služby ...), jsou písemně schváleny Zákazníkem. Účty k těmto službám jsou vytvořeny na správcovský účet ve vlastnictví Zákazníka a Dodavatel má k těmto službám (pokud je třeba) nasdílen přístup na svůj samostatný účet.

3.15.2. Návštěvnost webů je měřena a analyzována pomocí Google Analytics. Případné pokročilé měření nad rámec základních měřících kódů je součástí funkčních požadavků - např. Measurement Protocol či uživatelské interakce (události) negenerující zobrazení nové stránky (jako je třeba spuštění YouTube videa).

3.15.3. Na jednotlivé weby je možné v případě požadavku Zákazníka nasadit Google Tag Manager nebo obdobnou technologii. Zákazník určil, kdo za tag manager odpovídá.

4. POŽADAVKY NA DOKUMENTACI

4.1. Obecné

4.1.1. Veškerá technická, uživatelská či business dokumentace je v češtině.

4.1.2. Veškerá dokumentace je tvořena tak, aby podporovala potřeby Zákazníka pro bezpečnostní, technické a další audity a kontroly veřejnými i soukromými společnostmi a orgány.

4.1.3. Správnost a úplnost veškeré dokumentace dle této kapitoly je kontrolována a aktualizována minimálně 1x ročně a dále nejdříve dva měsíce a nejpozději týden před skončením platnosti Smlouvy.

4.2. Analýzy

4.2.1. Zákazník má k dispozici uspořádané a přehledné výstupy všech provedených analýz.

4.3. Návrhová a vývojářská dokumentace

4.3.1. Dodavatel předal Zákazníkovi vývojářskou dokumentaci v písemné podobě, obsahující minimálně:

a. Popis základní logiky/filozofie produktu.

b. Popis logické architektury systému, všech jeho komponent a jejich vazeb včetně diagramů.

c. Dokumentace návrhu databáze.

d. Popis klíčových aplikačních entit a jejich vztahů

e. Dokumentace všech implementovaných síťových API (typicky RPC, REST, JSON API, GraphQL, SOAP, apod.)

f. Definice coding standards.

g. Popis release procesu.

h. Popis verzovacího workflow.

i. Testovací scénáře.

4.4. Provozní dokumentace

4.4.1. Dodavatel předal Zákazníkovi dokumentaci v písemné podobě, obsahující minimálně:

a. Dokumentace kompletní infrastruktury a repository s šablonami pro automatické nastavení infrastruktury.

b. Detailní instalační manuál.

c. Popis případných změn v nastavení operačních systémů.

d. Popis konfigurace aplikačních a webových serverů a konfigurací databází.

e. Seznam externích služeb, závislostí a datových toků (např. Mailchimp, Sentry, DataDog, CRM, ERP apod.)

f. Dokumentace periodických procesů (typicky cron jobs).

g. Dokumentace k používaným automatizacím (hooks, makefiles, playbooks, ...)

h. Dokumentace k zabezpečení, zejména pro účely auditů

- dokumentace k VPN
- způsob ukládání hesel
- politika práce s klíči a certifikáty
- seznam osobních údajů, se kterými systém pracuje
- diagram, kudy putují osobní údaje systémem a kde jsou uložena
- seznam třetích stran, které mají přístup k osobním datům a smlouvy s těmito stranami

i. Dokumentace typů zasílaných e-mailů a způsobu jejich posílání (SMTP servery či služby a jejich požadavky na DNS záznamy).

j. Seznam standardních provozních úkonů a pracovních postupů pro správu systému.

k. Dokumentace k integracím či importům dat z externích zdrojů.

l. Detailní popis řešení zálohování a obnovy, včetně kompletních postupů Disaster Recovery. Dodavatel vytvořil a dále udržuje stále aktuální dokumentaci jednoznačně upravující kroky vedoucí k zajištění plné obnovy systému po havárii mající globální dopad na chod systému s ohledem na minimalizaci škod. Dokumentace DRP (Disaster Recovery Plan) je zpracována do nejmenšího detailu, to znamená vytvoření detailního postupu obnovy každé komponenty včetně popisu všech kroků vedoucí k její obnově. Pravidla zálohování obsahují vždy alespoň:

- specifikaci zálohovaných komponent (co je nutné zálohovat?)
- způsob jejich zálohování včetně časové návaznosti jednotlivých komponent (jakým způsobem se záloha má realizovat?)
- periodu zálohování (kdy / jak často se má záloha provádět?)
- retenční pravidla pro dobu a počet verzí uchovávaných záloh (jak dlouho a kolik verzí záloh se má uchovávat?)

m. Seznam administrátorských a servisních účtů k použitým operačním systémům, aplikacím a databázím.

n. Popis nastavení monitoringu a dohledu včetně použitých alertů a jejich konfigurace,

o. V samostatném dokumentu jsou evidovány metriky SLI a způsob jejich měření.

4.5. Bezpečnostní dokumentace

4.5.1. Dodavatel předal Zákazníkovi bezpečnostní dokumentaci v písemné podobě, minimálně v rozsahu:

a. Dokumentace k zabezpečení (VPN, ukládání hesel, popis použitých kryptografických prostředků atp.) zejména pro účely auditů.

b. Tabulka požadovaných síťových prostupů, ke každé povolené komunikaci obsahuje alespoň:

- Zdrojová adresa / Skupina adres
- Cílová adresa / Skupina adres
- Cílový komunikační port / Skupina komunikačních portů

- Poznámka (Stručný text důvodu komunikace)

c. Seznam všech použitých TLS certifikátů s dobou platnosti včetně popisu a podrobného postupu pro jejich obnovu.

4.6. Uživatelská a business dokumentace

4.6.1. Dodavatel předal Zákazníkovi uživatelskou dokumentaci v písemné podobě, obsahující minimálně:

a. Návod na zadávání a úpravu obsahu. Může odkazovat na dokumentaci použitého CMS (DMS, PIM, atp.) Může mít formu webové stránky dostupné přímo z rozhraní aplikace.

b. Dokumentace pro administrátorské role aplikace, včetně popisu správy uživatelů, rolí a jejich oprávnění.

5. Sledované ukazatele

5.1. Obecné

5.1.1. V samostatném provozním dokumentu budou definovány SLI (Service Level Indicators - vyhodnocované metriky) a k nim příslušné SLO (Service Level Objectives - cíle dosahovaných SLI, většinou jako minimální či maximální hodnota, popř. rozsah hodnot - typicky za udaný čas). U testování rychlosti pomocí webpagetest.org zahrnuje SLO region, z jakého je prováděn test.

5.1.2. Dodavatel zajišťuje měření a vyhodnocování jednotlivých SLI.

5.1.3. V dokumentu jsou definovány typy sledovaných stránek (např. homepage, landing page, hledání, ...) a konkrétní sledovaná URL pro související SLI.

5.1.4. Dokument SLI/SLO byl odsouhlasen před zahájením fáze 6 - Předání do pilotního provozu.

5.1.5. SLO uvedené tučně jsou minimální hodnoty v okamžiku uzavírání Smluv, po dohodě může být upraveno v dokumentu SLI/SLO. Pokud jsou nové hodnoty mírnější, je změna SLO písemně oddůvodněna.

5.2. Dostupnost

5.2.1. Dodavatel zajišťuje dodržení **minimální dostupnosti webů 99.5 % a administrace 95 %** měsíčně. Dodavatel není odpovědný za nedostupnost způsobenou nefunkčností infrastruktury či prostředků, které zajišťuje Zákazník, pokud dodrží Reakční lhůty.

5.2.2. Dosažená Dostupnost v procentech se vypočítá za každý kalendářní měsíc tak, že celkový počet celých minut, po který byla služba dostupná nebo probíhala plánovaná údržba v servisním okně, se vydělí celkovým počtem minut v měsíci a vynásobí 100. Pokud je mezi

samostatnými nedostupnostmi období kratší než 10 minut, považuje se toto celé období za nedostupnost.

5.3. Zátěž

5.3.1. Systém je realizován tak, že je připraven na současné používání **250 návštěvníků a 50 administrátorů** bez zaznamenatelného poklesu rychlosti. Web musí být funkční i při současném používání **500 návštěvníky a 100 administrátory**. V tomto případě je akceptovatelné **navýšení rychlosti odezvy až na 300 %**, nicméně web i administrace jsou stále použitelné pro práci.

5.4. Rychlost

5.4.1. Jako referenční prostředí pro desktopové měření rychlosti se považuje:

a. Prohlížeč Google Chrome v poslední stabilní verzi
b. Velikost displeje 1920x1280 (1080p, Full HD)
c. Konektivita Cable (5/1 Mbps 28ms RTT)

5.4.2. Pro celý "origin" Google Core Web Vitals, pokud jsou dostupná data v CrUX - **pass Core Web Vitals assessment.**

5.4.3. Pro vyjmenovaná typizovaná URL získávaná GET metodou

a. Core Web Vitals (LCP, FID, CLS) - **(good - "all green"**)
b. Google PageSpeed Insights Score Mobile / Desktop **(80/80)**
c. TTFB (Time To First Byte) **(max. 350 ms)**

5.5. Ostatní

a. Qualys SSL Labs Test Grade **(A)**
b. Securityheaders.com Grade **(C)**
c. Mozilla Observatory Grade **(D)**
d. RTO (recovery time objective) **(168 hodin)**
e. RPO (recovery point objective) **(24 hodin)**
f. Četnost HTTP chyb 50x **(max 0.02 % celý systém)**