ТЕХНИЧЕСКО ЗАДАНИЕ

за

Изграждане и внедряване на Специализирана автоматизирана информационна система за поддържане на регистрите в КЗЛД

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

1.1. Използвани акроними

Акроним	Описание
АИС	Автоматизирана информационна система
АЛД	Администратор на лични данни
АМС	Администрация на Министерския съвет
АОП	Агенция по обществени поръчки
АПК	Административнопроцесуален кодекс
БУЛСТАТ	Регистър Булстат
ДАЕУ	Държавна агенция "Електронно управление"
ДЛЗД	Длъжностно лице по защита на данните
ЗДОИ	Закон за достъп до обществена информация
ЗЕДЕП	Закон за електронния документ и електронния подпис
ЗЕУ	Закон за електронното управление
ЗЗЛД	Закон за защита на личните данни
ИТ	Информационни технологии
КАО	Комплексно административно обслужване
КЗЛД	Комисия за защита на личните данни
ТР	Търговски регистър
ДХЧО	Държавен хибриден частен облак
ЦАИС	Централизирана автоматизирана информационна система
SDK	Software development kit
API	Application programming interface/Приложно програмен интерфейс

1.2. Технологични дефиниции

Термин	Описание
Виртуална комуникационна инфраструктура	Инфраструктура, която на база съществуваща физическа свързаност, предоставена от ДАЕУ, предоставя възможност за изграждане на отделни и защитени виртуални мрежи за всяка една от структурите в сектора, при гарантиране на сигурен и защитен обмен на информация в тях.
Държавен хибриден частен облак	Централизирана на ниво държава информационна инфраструктура (сървъри, средства за съхранение на информация, комуникационно оборудване, съпътстващо оборудване, разпределени в няколко локации, в помещения отговарящи на критериите за изграждане на защитени центрове за данни), която предоставя физически и виртуални ресурси за ползване и администриране от секторите и структурите, които имат достъп до тях, в зависимост от нуждите им, при гарантиране на високо ниво на сигурност, надеждност, изолация на отделните ползватели и невъзможност от намеса в работоспособността на информационните им системи или неоторизиран достъп до информационните им ресурси. Изолацията на ресурсите и мрежите на отделните секторни ползватели (е-Общини, е-Правосъдие, е-Здравеопазване, е-Полиция) се гарантира с подходящи мерки на логическо ниво (формиране на отделни клъстери, виртуални информационни центрове и мрежи) и на физическо ниво (клетки и шкафове с контрол на достъпа).
Софтуер с отворен код	Компютърна програма, която се разпространява при условия, които осигуряват безплатен достъп до програмния код и позволяват: Използването на програмата и производните на нея компютърни програми, без ограничения в целта; Промени в програмния код и адаптирането на компютърната програма за нуждите на нейните ползватели; Разпространението на производните компютърни програми при същите условия. Списък на стандартни лицензионни споразумения, които предоставят тези възможности, който може да бъде намерен в подзаконовата нормативна уредба към Закона за електронно управление или на: http://opensource.org/licenses.

Машинночетим формат	Формат на данни, който е структуриран по начин, по който, без да се преобразува в друг формат позволява софтуерни приложения да идентифицират, разпознават и извличат специфични данни, включително отделни факти и тяхната вътрешна структура.
Отворен формат	Означава формат на данни, който не налага употребата на специфична платформа или специфичен софтуер за повторната употреба на съдържанието и е предоставен на обществеността без ограничения, които биха възпрепятствали повторното използване на информация.
Метаданни	Данни, описващи структурата на информацията, предмет на повторно използване.
Официален отворен стандарт	Стандарт, който е установен в писмена форма и описва спецификациите за изискванията как да се осигури софтуерна оперативна съвместимост.
Система за контрол на версиите	Технология, с която се създава специално място, наречено "хранилище", където е възможно да се следят и описват промените по дадено съдържание (текст, програмен код, двоични файлове). Една система за контрол на версиите трябва да може: • Да съхранява пълна история - кой, какво и кога е променил по съдържанието в хранилището, както и защо се прави промяната; • Да позволява преглеждане разликите между всеки две съхранени версии в хранилището; Да позволява при необходимост съдържанието в хранилището да може да се върне към предишна съхранена версия; • Да позволява наличието на множество копия на хранилището и синхронизация между тях. Цялата информация, налична в системата за контрол на версиите за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, трябва да може да бъде достъпна публично, онлайн, в реално време.

Първичен регистър	Регистър, който се поддържа от първичен администратор на данни - административен орган, който по силата на закон събира или създава данни за субекти (граждани или организации) или за обекти (движими и недвижими) за първи път и изменя или заличава тези данни. Например Търговският регистър е първичен регистър за юридическите лица със стопанска цел, Имотният регистър е първичен регистър за недвижима собственост.

1.3. Дефиниции за нива на електронизация на услугите

Термин	Описание
Ниво 1	Информация - предоставяне на информация за административни услуги по електронен път, включително за начини и места за заявяване на услугите, срокове и такси.
Ниво 2	Едностранна комуникация - информация съгласно дефиницията за Ниво 1 и осигурен публичен онлайн достъп до шаблони на електронни формуляри.
Ниво 3	Двустранна комуникация - заявяване и получаване на услуги изцяло по електронен път, включително електронно подаване на данни и документи, електронна обработка на формуляри и електронна персонална идентификация на потребителите.
Ниво 4	Извършване на сделки или транзакции по услуги от Ниво 3, включващи онлайн разплащане или доставка.

2. ВЪВЕДЕНИЕ

2.1. Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на обществена поръчка с предмет: „Изграждане и внедряване на Специализирана автоматизирана информационна система за поддържане на регистрите в КЗЛД“.

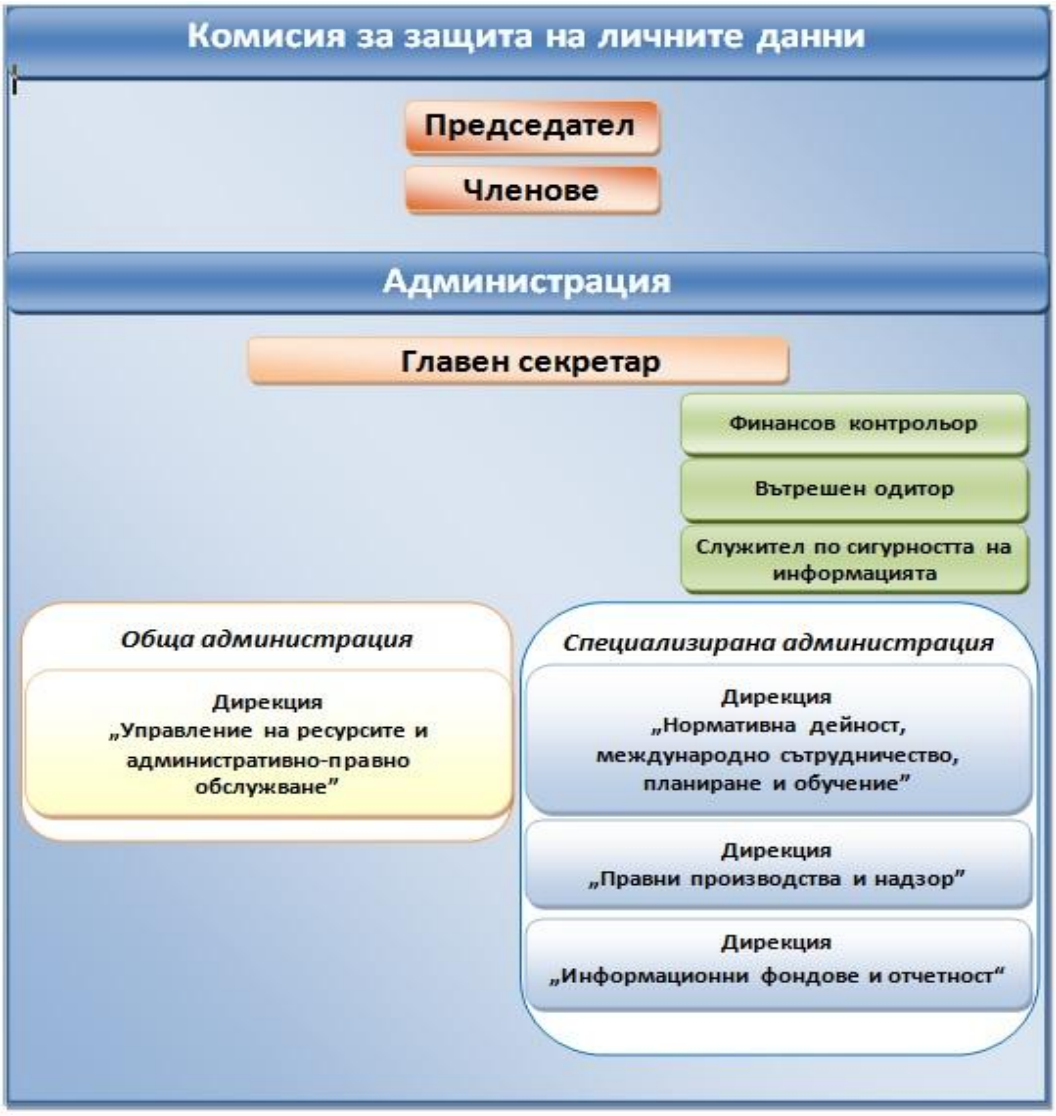
В настоящото техническо задание са описани и изискванията към проектната организация, документацията и отчетността.

2.2. За Възложителя - функции и структура

Комисията за защита на личните данни (КЗЛД) е единственият национален орган в Република България с контролни и надзорни правомощия в областта на защитата на личните

данни и личната неприкосновеност. По силата на Закона за защита на личните данни Комисията осъществява контрол както върху частно-правните субекти, така и върху публичните органи, когато същите действат като администратори на лични данни. Един от основните инструменти за превенция и установяване на единни стандарти сред администраторите на лични данни от частния и публичния сектор е провеждането на обучение. Това задължение е вменено на КЗЛД със Закона за защита на личните данни (чл. 10 ал. 13). В тази връзка за периода 2010 г.- 2016 г. експертите на Комисията са провели над 110 семинара, на които са обучени над 2000 души от публичния и частния сектор.

Структурата на Комисията за защита на личните данни е представена във Фигура 1:



Фигура 1. Структура на Комисия за защита на личните данни

2.3. За проекта

Общият регламент относно защитата на данните (РЕГЛАМЕНТ (ЕС) 2016/679) влиза в сила от 25.05.2018 г. Същият е задължителен в своята цялост, прилага се пряко във всички държави членки и цели изграждането на единна за ЕС система за защита на личните данни, отговаряща на съвременната реалност, свързана с развитието на информационните

технологии.

Изискванията на Общия регламент и промените в националното законодателство (ЗЗЛД) налагат Комисията за защита на личните данни, в качеството и на постоянно действащ национален надзорен орган в областта на защита на личните данни, да изгради и да поддържа нови регистри, по-голямата част от които са публични.

2.4. Нормативна рамка

Проектът се осъществява в съответствие с изискванията, регламентирани със следните нормативни актове и стратегически документи:

- РЕГЛАМЕНТ (ЕС) 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/БО (Общ регламент относно защитата на данните);
- ЗАКОН ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.

3. Цели, обхват и очаквани резултати от изпълнение на проекта

3.1. Общи и специфични цели на проекта

Привеждане на системата за защита а личните данни в Р. България в съответствие с нормативните изисквания на Общия регламент относно защитата на данните, ЗЗЛД и актовете по тяхното прилагане.

Постигането на общата цел ще бъде реализирано чрез следните специфични цели, съответстващи на планираните по проекта дейности:

- Повишаване информираността на гражданите и бизнеса (АЛД и ДЛЗД) относно правата и задълженията, произтичащи от нормативната база. Формулиране на ясни и конкретни насоки в процесите по защита на личните данни.
- Улесняване на контакта на гражданите с ДЛЗД и достъпа до техните лични данни.
- Облекчаване на АЛД при търсене на услуги от ДЛЗД. Гарантиране на пряка връзка на КЗЛД с ДЛЗД, както и възможност за извършване на анализи и статистики относно тяхната дейност, профили и т.н. По-добър контрол върху работата им.
- Регистърът на сертифициращите органи, акредитирани от КЗЛД, ще бъде в помощ на АЛД, които желаят да се сертифицират. Ще даде прозрачност на процедурата по акредитиране на сертифициращи органи.

- Публикуването на Кодексите на поведение ще е в помощ на АЛД и ДЛЗД по отношение спазването на нормативните изисквания (основни насоки, конкретни действия по защита на данните, добри практики и т.н.).
- Системата за уведомяване за пробив в сигурността ще улесни и съкрати времето за подаване на тези уведомления. Ще има възможност за статистика и анализ на пробивите в сигурността – установяване на слаби места в системата за защита, атакуеми сфери (по АЛД, секторно).

3.2. Обхват на проекта

Описаните в т. 3.1 цели се осъществяват с изпълнението на следните основни дейности, които формират обхвата на проекта:

- Създаване и поддържане на Регистър на длъжностните лица по защита на данните (ДЛЗД).
- Създаване и поддържане на Регистър на акредитирани, сертифициращи организации (АСО).
- Създаване и поддържане на Регистър на кодекси за поведение (КП).
- Осигуряване на публична част на гореизброените регистри.
- Създаване и поддържане на Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия - Регистър на нарушенията и предприетите мерки (НПМ).

3.3. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

- Граждани и бизнесът, както и други лица, осъществяващи публични функции.
- Комисия за защита на личните данни.
- Администратори и обработващи лични данни.
- Длъжностни лица по защита на данните.

3.4. Очаквани резултати

Очакваните резултати от изпълнението на настоящата поръчка са постигане на общите и специфични цели, описани в т. 3.1.

3.5. Период на изпълнение

Периодът на изпълнение е [X] месеца, но не по късно от [ДД.ММ.ГГГГ] г. Участниците трябва да изготвят подробен график, в който следва да се конкретизират сроковете за изпълнение на всяка дейност и поддейност от настоящата поръчка. Графикът за изпълнение трябва да бъде съобразен с продължителността на дейността и не може да надвишава [X]

месеца от дата на сключване на договора.

4. ТЕКУЩО СЪСТОЯНИЕ

Изграждането и поддържането на посочените регистри е ново задължение за КЗЛД, поради което към настоящия момент няма установена практика и натрупан опит в тази сфера.

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

5.1. Изисквания към екипа за изпълнение на обществената поръчка

Минималните изисквания към екипа за изпълнение на обществената поръчка, както следва:

За Ръководител проект:

Образование: висше образование, степен „магистър“ в област „Технически науки“ или „Природни науки, математика и информатика“ или еквивалент;

Професионален опит: да е бил ръководител и да е извършил анализ на бизнес процеси на най-малко 2 (две) успешно приключени дейности с предмет, включващ разработка и внедряване на уеб базирана информационна система;

За Системен архитект:

Образование: висше образование, степен „магистър“ в област „Технически науки“ или „Природни науки, математика и информатика“ или еквивалент;

Професионален опит: да е проектирал архитектурата на система в рамките на най-малко 2 (две) успешно приключени дейности с предмет, включващ разработка и внедряване на уеб базирана информационна система.

За Бизнес анализатор:

Образование: висше образование, степен „магистър“ в област „Технически науки“ или „Природни науки, математика и информатика“ или еквивалент;

Професионален опит: да е извършил описването на бизнес процеси, бизнес анализ и моделиране на процеси в областта на информационни системи и технологии, в т.ч. в сферата на електронно управление.в рамките на най-малко 2 (две) успешно приключени дейности с предмет, включващ разработка и внедряване на уеб базирана информационна система.

За Програмист – 3 броя:

Образование: висше образование, степен „магистър“ в област „Технически науки“ или „Природни науки, математика и информатика“ или еквивалент;

Професионален опит: да е участвал в проектиране и разработка на информационни системи в рамките на най-малко 2 (две) успешно приключени дейности с предмет, включващ разработка и внедряване на уеб базирана информационна система.

За Специалист осигуряване на качеството (QA) - 2 броя:

Образование: висше образование, степен „магистър“ в област „Технически науки“ или „Природни науки, математика и информатика“ или еквивалент;

Професионален опит: да е участвал в планиране и управление на процеса и дейностите по осигуряване на качеството чрез методика за тестване и разработване на инструменти и управление на инциденти в рамките на най-малко 2 (две) успешно приключени дейности с предмет, включващ разработка и внедряване на уеб базирана информационна система.

5.2. Общи организационни принципи

Задължително изискване е да се спазят утвърдените хоризонтални и вертикални принципи на организация на изпълнението на предмета на обществената поръчка за гарантирано постигане на желаните резултати от проекта, така че да се покрие пълният набор от компетенции и ноу-хау, необходими за изпълнение на предмета на поръчката, а също така да се гарантира и достатъчно ниво на ангажираност с изпълнението и проблемите на проекта:

- Хоризонталният принцип предполага ангажиране на специалисти от различни звена, така че да се покрие пълният набор от компетенции и ноу-хау по предмета на проекта и същевременно екипът да усвои новите разработки на достатъчно ранен етап, така че да е в състояние пълноценно да ги използва и развива и след приключване на проекта;
- Вертикалният принцип включва участие на експерти и представители на различните управленски нива, така че управленският екип да покрива както експертните области, необходими за правилното и качествено изпълнение на проекта, така и управленски и организационни умения и възможности за осъществяване на политиката във връзка с изпълнението на проекта. Чрез участие на ръководители на звената - ползватели на резултата от проекта, ще се гарантира достатъчно ниво на ангажираност на институцията с проблемите на проекта.

5.3. Управление на проекта[1]

Дейностите по управление на проекта трябва да включват като минимум управление на реализацията на всички дейности, посочени в настоящата обществена поръчка, и постигане на очакваните резултати, както и разпределението на предложените участници в екипа за управление на поръчката по роли, график и дейности при изпълнение на настоящата обществена поръчка.

Доброто управление на проекта трябва да осигури:

- координиране на усилията на експертите от страна на Изпълнителя и Възложителя и осигуряване на висока степен на взаимодействие между членовете на проектния екип;
- оптимално използване на ресурсите;

[1] Под „проект“ следва да се разбира предметът на обществената поръчка.

- текущ контрол по изпълнението на проектните дейности;
- разпространяване навреме на необходимата информация до всички участници в проекта;
- идентифициране на промени и осигуряване на техните анализ и координация;
- осигуряване на качеството и полагане на усилия за непрекъснато подобряване на работата за удовлетворяване на изискванията на участниците в проекта.

Методологията трябва да включва подробно описание на:

- фазите на проекта;
- организация на изпълнение:
  - структура на екипа на Изпълнителя;
  - начин на взаимодействие между членовете на екипа на Изпълнителя;
  - връзки за взаимодействие с екипа на Възложителя;
- проектна документация:
  - видове доклади;
  - техническа и експлоатационна документация;
  - време на предаване;
  - съдържание на документите;
  - управление на версиите.
- управление на качеството;
- график за изпълнение на проекта.

В графика участниците трябва да опишат дейностите и стъпките за тяхното изпълнение максимално детайлно, като покажат логическата връзка между тях. В графика трябва да са посочени датите за предаване на всеки от документите, изготвени в изпълнение на обществената поръчка.

5.4. Управление на риска

В техническото си предложение участниците трябва да опишат подхода за управление на риска, който ще прилагат при изпълнението на поръчката.

Участниците трябва да представят и списък с идентифицираните от Възложителя рискове с оценка на вероятност, въздействие и мерки за реакция.

През времето за изпълнение на проекта Изпълнителят трябва да следи рисковете, да

оценява тяхното влияние, да анализира ситуацията и да идентифицира (евентуално) нови рискове.

В хода на изпълнение на поръчката Изпълнителят следва да поддържа актуален списък с рисковете и да докладва състоянието на рисковете най-малко с месечните отчети за напредъка.

При изготвянето на списъка с рискове Участниците следва да вземат предвид следните идентифицирани от Възложителя рискове:

- Промяна в нормативната уредба, водеща до промяна на ключови компоненти на решението - предмет на разработка на настоящата обществена поръчка;
- Недобра комуникация между екипите на Възложителя и Изпълнителя по време на аналитичните етапи на проекта;
- Ненавременно изпълнение на всяко от задълженията от страна на Изпълнителя;
- Неправилно и неефективно разпределяне на ресурсите и отговорностите при изпълнението на договора;
- Забавяне при изпълнение на проектните дейности, опасност от неспазване на срока за изпълнение на настоящата поръчка;
- Грешки при разработване на функционалностите на системата;
- Недостатъчна яснота по правната рамка и/или променяща се правна рамка по време на изпълнение на проекта;
- Липса на задълбоченост при изследването и описанието на бизнес процесите и данните;
- Неинформиране на Възложителя за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на дейностите;
- Риск за администриране на системата след изтичане на периода на гаранционна поддръжка.

6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА

В техническото си предложение участниците трябва да предложат подход за изпълнение на проекта, като включат минимум следните етапи:

6.1. Анализ на данните и изискванията

Функционален обхват на проекта

Разработка и внедряване на нови вътрешни и публичен регистри.

Независимо от източника на финансиране са приложими и предварителните условия за

допустимост (Приложение № 1 от Пътната карта за електронно управление 2016-2020) за финансиране на проекти по ОП „Добро управление”, в т.ч.:

- Предвидените за разработка и внедряване услуги трябва да бъдат регистрирани предварително в Регистъра на услугите към Административния регистър (съгласно чл. 61 от Закона за администрацията) и да бъдат въведени и валидирани данни за броя на транзакциите по предоставяне на тези услуги в Модула „Самооценка на административното обслужване" в Интегрираната информационна система на държавната администрация (ИИСДА). Услугите, които ще бъдат надградени, и новоразработените услуги трябва да отговарят на изискванията за електронни услуги с минимално Ниво 4, където е приложимо (т.е. услугата изисква заплащане на такса), или Ниво 3, в случаите, в които за предоставяне на услугата не се изисква заплащане на такса; Дефинициите за нивата на електронизация на административните услуги са регламентирани в Наредбата за административния регистър към Закона за администрацията;

- В процеса на бизнес анализ да бъдат изследвана съвместимостта на бизнес процесите на Възложителя с вече одобрени оптимизирани референтни модели за предоставяне на услуги и нормативни изисквания на Базисен модел за Комплексно административно обслужване в държавната администрация. При наличие на разработени модели за предоставяне на услуги по „Епизоди от живота" и „Събития от бизнеса", които включват услуги, предоставяни от Възложителя, да бъдат съобразени нуждите от модификации в референтните модели, за да се постигне подобряване на времето и намаляване на административната тежест при комплексно обслужване, спрямо предоставянето на отделните услуги поединично;

- В случай че се касае за административни услуги, те трябва да бъдат разграничени на базата на разлики в бизнес процесите и да не бъдат генерализирани и/или обобщавани на базата на типа на действие (например ако Системата издава няколко различни вида удостоверения, с които се удостоверяват различни обстоятелства, административните услуги трябва да бъдат регистрирани отделно);

- Удостоверителните административни услуги трябва да бъдат регистрирани и като вътрешни административни услуги и да бъде реализирана възможност за предоставянето на тези услуги като електронни вътрешно- административни услуги за нуждите на комплексното административно обслужване чрез служебен онлайн интерфейс.

6.2. Специфични изисквания към етапите на бизнес анализа и разработка

- Изпълнителят трябва да следва Методологията за усъвършенстване на работните процеси за предоставяне на административни услуги и Наръчника за прилагане на методологията, приета с Решение № 578 на Министерския съвет от 30 септември 2013 г.;

- Трябва да бъде предвидена фаза на проучване, по време на която да се дефинират потребителските нужди, да се проведат предварителни тестове с потребители и да се изработи план, по който да се адресират идентифицираните нужди;
- Трябва да бъдат предвидени периодични продуктови тествания по време на разработката и внедряването на Системата, с извадка (фокус-група) от бъдещите потребители на електронната услуга (служители в администрацията, граждани, доставчици на обществени услуги), чрез които да се изпита и оцени използваемостта на услугите и потребителските интерфейси, както и за да бъдат отстранени затруднения и несъответствия със заданието;
- Трябва да се спазват нормативните изисквания за еднократно събиране и повторна употреба на данни в държавната администрация (съгласно АПК и ЗЕУ) и в разработените бизнес процеси да не се изискват данни за заявителя и/или за получателя на услугата, които могат да се извлекат автоматично в процеса на електронна идентификация чрез Центъра за електронна идентификация или на база на ЕГН от КЕП. При необходимост изпълнителят трябва да предложи на Възложителя адекватни промени в нормативната уредба, които да хармонизират съответните секторни нормативни изисквания с общите разпоредби на Административнопроцесуалния кодекс, Закона за електронно управление, Закона за електронния документ и електронния подпис и приложимите подзаконови актове, ако действащата нормативна уредба изисква:
  - изрично попълване на типов хартиен формуляр, върху който потребителите трябва да се подпишат собственоръчно и/или който да приложат като изискуем документ при заявяването на електронна административна услуга;
  - изрично деклариране или обявяване на обстоятелства или данни, които се администрират и/или удостоверяват от други държавни органи и могат да бъдат получени по служебен път, включително и автоматизирано през съответни интеграционни интерфейси;
  - други нормативни изисквания, които водят до неоптимални или ненужно бюрократични процеси, които биха могли да бъдат оптимизирани при заявяване и предоставяне на електронни административни услуги;
- При оптимизацията на потребителския път трябва да се отчита всяко действие от страна на потребителя (натискане на бутон, въвеждане на данни, прочитане на текст и пр.), което може да се спести.

6.3. Специфични изисквания при оптимизиране на процесите по заявяване на електронни административни услуги в зависимост от заявителя

Неприложимо**.**

6.4. Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила

Неприложимо**.**

6.5. Изисквания към регистрите и предоставянето на административните услуги

Неприложимо.

6.6. Изготвяне на системен проект

Изпълнителят трябва да изготви системен проект, който подлежи на одобрение от Възложителя. В системния проект трябва да са описани всички изисквания за реализирането на Системата. Изготвянето на системния проект включва следните основни задачи:

- Определяне на концепция на информационната система на базата на техническото задание;
- Дефиниране на детайлни изисквания и бизнес процеси, които трябва да се реализират в Системата;
- Дизайн на информационната система, хардуерната и комуникационната инфраструктура;
- Изготвяне на план за техническа реализация;
- Определяне на потребителския интерфейс.

Изпълнението на задачите изисква дефиниране на модели на бизнес процеси, модели на стандартни справки и анализи, модели на печатни бланки, политика за сигурност и защита на данните, основни изграждащи блокове, транзакции, технология на взаимодействие, мониторинг на системата, спецификация на номенклатурите, роли в системата и други. При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва стандартен език за описание на бизнес процеси - BPMN.

Системният проект подлежи на одобрение от Възложителя. В случай на забележки, корекции или допълнения от страна на Възложителя Изпълнителят е длъжен да ги отрази в системния проект в срок не по-късно от 5 (пет) работни дни.

6.7. Разработване на софтуерното решение

Етапът на разработка включва изпълнението на следните задачи:

- *[ако е приложимо]* Разработка на прототип, който трябва да бъде одобрен от Възложителя и въз основа, на който трябва да се разработи цялата система;
- Разработка на модулите на информационната система съгласно изискванията на настоящото техническо задание и системния проект;
- Провеждане на вътрешни тестове на Системата (в среда на разработчика);
- Изготвяне на детайлни сценарии за провеждане на приемателните тестове за етапи „Тестване” и „Внедряване” на проекта.

За изпълнение на дейностите по разработка на системата участниците в настоящата обществена поръчка трябва да опишат в своите технически предложения приложим подход (методология) за софтуерна разработка, която ще използват, както и инструментите за разработка и средата за провеждане на вътрешните тестове. Участниците трябва да опишат как предложеният от тях подход ще бъде адаптиран за успешната реализация на Системата.

6.8. Тестване

Изпълнителят трябва да проведе тестване на софтуерното решение в създадена за целта тестова среда, за да демонстрира, че изискванията са изпълнени. Изпълнителят трябва да предложи и опише методология за тестване, която ще използва в план за тестване с описание на обхвата на тестването, вид и спецификация на тестовете, управление на дефектите, регресионна политика, инструменти, логистично осигуряване и други параметри на процеса.

6.9. Внедряване

Изпълнителят трябва да внедри софтуерното решение в информационната и комуникационна среда на КЗЛД. Това включва инсталиране, конфигуриране и настройка на програмните компоненти на системата в условията на експлоатационната среда на КЗЛД.

6.10. Обучение

Изпълнителят трябва да организира и да проведе обучения за следните групи и ползватели на софтуерното решение:

- Администратори на системата;
- Потребители;

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка:

- Необходимия хардуер;
- Необходимия софтуер;
- Учебни материали;
- Лектори.

6.11. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от минимум 24 (двадесет и четири) месеца след приемане в експлоатация на системата.

При необходимост, по време на гаранционния период трябва да бъдат осъществявани дейности по осигуряване на експлоатационната годност на софтуера и ефективното му използване от Възложителя, в случай че настъпят явни отклонения от нормалните експлоатационни характеристики, заложени в системния проект.

Изпълнителят следва да предоставя услугите по гаранционна поддръжка, като предоставя за своя сметка единна точка за достъп за приемане на телефонни и e-mail съобщения.

Приоритетите на проблемите се определят от Възложителя в зависимост от влиянието им върху работата на администрацията. Редът на отстраняване на проблемите се определя в

зависимост от техния приоритет.

Минималният обхват на поддръжката трябва да включва:

- Извършване на диагностика на докладван проблем с цел осигуряване на правилното функциониране на системите и модулите;
- Отстраняване на дефектите, открити в софтуерните модули, които са модифицирани или разработени в обхвата на проекта;
- Консултации за разрешаване на проблеми по предложената от Изпълнителя конфигурация на средата (операционна система, база данни, middleware, хардуер и мрежи), използвана от приложението, включително промени в конфигурацията на софтуерната инфраструктура на мястото на инсталация;
- Възстановяването на системата и данните при евентуален срив на системата, както и коригирането им в следствие на грешки в системата;
- Експертни консултации по телефон и електронна поща за системните администратори на Възложителя за идентифициране на дефекти или грешки в софтуера;
- Актуализация и предаване на нова версия на документацията на системата при установени явни несъответствия с фактически реализираните функционалности, както и в случаите, в които са извършени действия по отстраняване на дефекти и грешки, в рамките на гаранционната поддръжка.

7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

7.1. Функционални изисквания към информационната система

Комисията за защита на личните данни (КЗЛД) поддържа следните регистри:

Публични регистри:

- Регистър на длъжностните лица по защита на данните;
- Регистър на акредитирани сертифициращи организации;
- Регистър на кодекси за поведение.

Непублични:

- Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия (Регистър на нарушенията и предприетите мерки).

Регистрите се поддържат с помощта на специализирана автоматизирана информационна система (САИС).

Общи функционални изисквания към САИС:

- Да поддържа два режима на работа – публичен и непубличен;
- Да осигурява идентификация и автентификация на потребителите при работа с данните (въвеждане, редактиране, заличаване);
- Да позволява динамично управление на потребители (създаване, присвояване/промяна на роли и привилегии, активиране/деактивиране);
- Да поддържа история на данните и на техните промени;
- Да поддържа одитни записи;
- Да дава възможност са генериране на справки.

Регистър на длъжностните лица по защита на данните (ДЛЗД)

Общо описание на регистър ДЛЗД.

Администраторът (АЛД) и обработващият лични данни определят длъжностно лице по защита на данните (ДЛЗД) във всички случаи, когато:

- обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни;
- е налице мащабно обработване на данни по чл. 5 ал. 1 от ЗЗЛД;
- обработването на лични данни е за целите на:
- отбраната на страната;
- националната сигурност;
- опазването на обществения ред и противодействието на престъпността;
- наказателното производство;
- изпълнението на наказанията (Доколкото в специален закон не е предвидено друго);
- обработва лични данни на над 10 000 физически лица.

ДЛЗД може да бъде определено и от сдружения, организации или други структури, представляващи категории администратори или обработващи лични данни.

Едно ДЛЗД може да бъде назначено за няколко АЛД/ОЛД/сдружения или организации (по-нататък само АЛД).

АЛД могат да определят повече от едно ДЛЗД.

Администраторът съобщава имената и данните за контакт на ДЛЗД на КЗЛД, както и последващи промени в тях и публикува координатите за връзка с него. Формата и съдържанието на уведомлението и реда за подаването му до Комисията се определят с

Правилника за дейността на Комисията и нейната администрация.

ДЛЗД, когато е в мандат, уведомява КЗЛД за промяна на всички обстоятелства свързани с АЛД, залегнали в Уведомлението.

Уведомлението се подава в КЗЛД по един от следните начини:

- По електронен път, при спазване на изискванията на Закона за електронния документ и електронния подпис:
- Въвеждане/промяна на данните с помощта на екранна форма на САИС;
- Електронна поща - електронно подписан прикачен файл.
- По пощата - на хартиен носител, в оригинал;
- В приемната на КЗЛД.

Предназначение на регистър ДЛЗД.

Предназначението на регистъра е да:

- подпомага КЗЛД при изпълнение на надзорните си задължения и правомощия;
- даде възможност на гражданите и на обществеността за контакт с ДЛЗД/АЛД.

Регистърът е електронен и е публичен.

Описание на данните в регистъра.

Данни за ДЛЗД

Данни за идентификация на ДЛЗД:

- Име, презиме и фамилия;
- ЕГН/ЛНЧ;
- Идентификационен номер в регистъра.

Данни за контакт с ДЛЗД (за конкретен АЛД):

- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

Други, допълнителни данни за ДЛЗД (за сега неструктурирани - свободен текст, например: данни за сертификати);

Данни за АЛД

Данни за идентификация на АЛД:

- Код по БУЛСТАТ/ЕИК;
- Име на АЛД;

* Представляващ/и АЛД - Име, презиме и фамилия;

- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к...).
- Адрес за кореспонденция - област, населено място, пощенски код, адрес;
- Адрес на интернет страница.

Други допълнителни данни за АЛД (за сега неструктурирани - свободен текст).

Ограничения

- Не всички данни от регистъра са публични;
- Във връзка с чл. 2 от Закона за електронното управление, АЛД/ДЛЗД подават само данни, които са достатъчни за тяхната еднозначна идентификация. КЗЛД получава останалата информация от съответния първичен администратор на данни, по един от следните начини:
  - Автоматично - обмен на заявки между САИС със системи на други организации (например Агенция по вписванията - ТР, РБУЛСТАТ);
  - Автоматизирано - служители на КЗЛД получават необходимата информацията от публични регистри на други организации и я въвеждат в системата.

Регистър на акредитирани, сертифициращи организации (АСО)

Общо описание на регистър АСО

С цел да се демонстрира спазването на Регламент 2016/679 и на Закона при операциите по обработване от страна на администраторите и обработващите лични данни, на същите могат да се издават сертификати.

Организации, притежаващи подходящ опит в областта на защитата на данните могат да издават, подновяват и прекратяват сертификати. Когато тези организации получат акредитация, същите се наричат сертифициращи органи.

Акредитацията на сертифициращи органи се извършва от Комисията за защита на личните данни въз основа на критерии, определени от нея или от Европейския комитет по защита на данните, или от водещия надзорен орган на друга държава членка - при трансгранично обработване на лични данни.

Акредитацията се издава за срок от пет години и може да бъде подновена от Комисията при същите условия.

Комисията за защита на личните данни анулира акредитацията на сертифициращ орган, когато установи, че вече не се спазват условията за акредитация, или че предприетите от сертифициращия орган действия нарушават Закона или Регламент (ЕС) 2016/679.

Критериите, механизмите и процедурите за сертифициран е, печати и маркировки се уреждат в наредба, издадена от Комисията за защита на личните данни. Наредбата се обнародва в „Държавен вестник”.

След извършване на процедурите по акредитация, сертифициращия орган получава сертификат за акредитация.

Регистърът е електронен и е публичен.

Предназначение на регистър АСО

Предназначението на регистъра е да осигури публичност на сертифициращите органи.

Описание на данните

Данни за идентификация на сертифициращия орган:

- Идентификационен номер в регистър АСО;
- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Наименование на организацията;
- Представляващ/и организацията - Име, презиме и фамилия;
- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к...).
- Адрес за кореспонденция:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к ...).
- Адрес на интернет страница.

Данни на лица за контакти:

- Име, презиме и фамилия;
- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

Данни за сертификата:

- Идентификационен номер;
- Дата на издаване на сертификата;
- Дата/Срок на валидност;
- Дата на анулиране на сертификата;
- Описание на причините за анулиране.

Ограничения

Не всички данни от регистъра са публични. Публичната част на регистъра се урежда с Наредбата по предходната точка.

Регистър на кодекси за поведение (КП)

Общо описание на регистър КП

Сдруженията и други структури, представляващи категории администратори или обработващи лични данни, могат да изготвят кодекси за поведение или да изменят или допълват такива кодекси с цел да бъде уточнено прилагането на Регламента и закона.

Изготвянето на кодекси за поведение има за цел да допринесат за правилното прилагане на регулаторната рамка, като се отчитат специфичните характеристики на различните АЛД и обработващи данни, по браншове и сектори.

Кодексите за поведение имат наблюдаващи органи. Наблюдаващият орган може да извършва промени в кодексите, за което информира КЗЛД.

КЗЛД одобрява или връща за доработка на проектите на кодексите за поведение. Одобрените кодекси са поведение се вписват в регистъра.

Регистърът е електронен и е публичен.

Предназначение на регистър КП

Регистърът е предназначен да осигури публичност на одобрените кодекси за поведение и техните наблюдаващи органи.

Описание на данните

Данни за кодексите

- Идентификационен номер в регистър КП;
- Наименование;
- Сектор/бранш;
- Дата на одобрение/публикуване;
- Дата на последна промяна;
- Дата на „заличаване“ в регистъра;
- Описание на обстоятелствата по заличаване.

Данни за издателя на кодекса

- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Наименование;
- Представляващ/и - име, презиме и фамилия;

- Седалище и адрес на управление:
    - област;
    - населено място;
    - пощенски код;
    - адрес (ул. №, ж.к...).
- Адрес за кореспонденция - област, населено място, пощенски код, адрес;
- Адрес на интернет страница.

Данни на лица за контакти:

- Име, презиме и фамилия;
- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

Данни за органа, акредитиран да наблюдава КП:

- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Наименование;
- Представляващ/и - Име, презиме и фамилия;
- Седалище и адрес на управление (ако е приложимо):
    - област;
    - населено място;
    - пощенски код;
    - адрес (ул. №, ж.к.).
- Адрес за кореспонденция - област, населено място, пощенски код, адрес;
- Адрес на интернет страница.

Ограничения

Не всички данни от регистъра са публични.

Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия - Регистър на нарушенията и предприетите мерки (НПМ)

Общо описание на регистър НПМ

В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо - не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на данните КЗЛД.

Уведомлението се подава в КЗЛД по един от следните начини:

- По електронен път, при спазване на изискванията на Закона за електронния документ и електронния подпис:

- Въвеждане/промяна на данните с помощта на екранна форма на САИС;
- Електронна поща - електронно подписан прикачен файл.

- По пощата - На хартиен носител, в оригинал;
- В приемната на КЗЛД.

Предназначение на регистър НПМ

Предназначението на регистъра е да:

- подпомага КЗЛД при изпълнение на надзорните си задължения и правомощия;
- дава възможност за анализи на причините за възникналите нарушение на сигурността на данните, с цел идентифициране на тенденции и евентуална превенция.

Регистърът е електронен и НЕ е публичен.

Описание на данните

Данни за идентификация на АЛД, обект на нарушението:

- Код по БУЛСТАТ/ЕИК (ако е приложимо);
- Име на АЛД;
- Представляващ/и АЛД - Име, презиме и фамилия;
- Седалище и адрес на управление:
  - област;
  - населено място;
  - пощенски код;
  - адрес (ул. №, ж.к...).

Данни за нарушението

- Тип на нарушението (ако е приложимо, да се избира от списък/класификатор на нарушенията);
- Описание на естеството на нарушението на сигурността на данните, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- Описание на евентуалните последици от нарушението на сигурността на личните данни;
- Описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици;
- Дата за събитието/събитията довели до нарушението на сигурността на личните данни (ако е приложимо);
- Дата на уведомяване на КЗЛД;
- Спазен ли е 72-часовия срок (ДА/НЕ);
- Описание на причините за забавянето, когато не е подадено в срок от 72 часа.

Данни за ДЛЗД или за друго лице за контакт:

- Име, презиме и фамилия;
- Телефонен;
- Мобилен телефон;
- Електронен адрес;
- Факс.

7.1.1. Интеграция с външни информационни системи

За реализиране на основни бизнес процеси Системата не трябва да поддържа интеграция в реално време с информационни системи на други администрации.

7.1.2. Интеграционен слой

Неприложимо.

7.1.3. Технически изисквания към интерфейсите

Приложните програмни интерфейси трябва да отговарят на следните архитектурни, функционални и технологични изисквания:

- Служебните онлайн интерфейси трябва да се предоставят като уеб-услуги (web-services) и да осигуряват достатъчна мащабируемост и производителност за обслужване на синхронни заявки (sync pull) в реално време, с максимално време за отговор на заявки под 1 секунда за 95% от заявките, които не включват запитвания до регистри и външни системи. Изпълнителят трябва да обоснове прогнозирано натоварване на Системата и да предложи критерии за оценка на максимално допустимото време за отговор на машинна заявка. Критерият за оценка следва да се основава на анализ на прогнозираното натоварване и на наличния хардуер, който ще се използва. Изпълнителят трябва да представи обосновано предложение за минималното време за отговор на заявка на базата на посочените по-горе критерии и да осигури нужните условия за спазването му;
- Трябва да се реализира интегриране на модул за разпределен кохерентен кеш (Distributed Caching) на „горещите данни", които Системата получава и/или които се обменят през служебните онлайн интерфейси, като логиката на Системата трябва гарантира кохерентност (Cache Coherency) между кешираните данни и данните, съхранявани в базите данни;
- Да бъде предвидено създаването и поддържането на тестова среда, достъпна за използване и извършване на интеграционни тестове от разработчици на информационни системи, включително такива, изпълняващи дейности за други администрации или за бизнеса, с цел по-лесно и устойчиво интегриране на съществуващите и бъдещи информационни системи.

7.1.4. Електронна идентификация на потребителите

- Електронната идентификация на всички потребители трябва да бъде реализирана в съответствие с изискванията на Регламент ЕС 910/2014 и Закона за електронната идентификация;
- Трябва да бъде реализирана интеграция с националната схема за електронна идентификация съгласно изискванията на Закона за електронната идентификация и действащите нормативни правила за оперативна съвместимост. За целта подсистемата за автентикация и оторизация на потребителите трябва да поддържа интеграция с външен доставчик на идентичност - в случая с Центъра за електронна идентификация към Държавна агенция „Електронно управление”. Реализацията на интеграцията трябва да бъде осъществена по стандартни протоколи SAML 2.0 и/или OpenID Connect;
- Системата трябва да поддържа и стандартен подход за регистрация на потребители с потребителско име и парола - за потребители, които нямат издадени удостоверения за електронна идентичност, и за потребители, които желаят да продължат да използват електронни административни услуги с КЕП;
- Процесът по регистрация на потребители трябва да бъде максимално опростен и бърз, но трябва да включва следните специфични стъпки:
    - Визуализиране на информация относно стъпките по регистрация и информация във връзка с процеса за потвърждаване на регистрацията и активиране на потребителския профил. Съвети към потребителите за проверка на настройките на имейл клиентите, свързани с блокиране на спам, и съвети за включване на домейна на Възложителя в "бял списък";
    - Избор на потребителско име с контекстна валидация на полетата (in-line validation), включително и за избраното потребителско име;
    - Избор на парола с контекстна валидация на полето (in-line validation) и визуализиране на сложността на паролата като „слаба”, „нормална” и „силна”;
    - Реализиране на функционалност за потвърждение и активиране на регистрацията чрез изпращане на съобщение до регистрирания имейл адрес на потребителя с хипер-линк, с еднократно генериран токън с ограничена времева валидност за потвърждение на регистрацията. Възможност за последващо препращане на имейла за потвърждение, в случай че е бил блокиран от системата на потребителя.
- При реализиране на вход в Системата с удостоверение за електронна идентичност, по Националната схема за електронна идентификация, Системата трябва да използва потребителския профил, създаден в Системата за електронна идентификация, чрез интерфейси и по протоколи съгласно подзаконовата нормативна уредба към Закона за електронната идентификация. В случай че даден потребител има регистриран потребителски профил в Системата, който е създаден преди въвеждането на Националната схема за електронна идентификация, Системата трябва да предлага на потребителя възможност за „сливане” на профилите и асоцииране на локалния профил с този от Националната система за електронна идентификация. Допустимо е

Системата да поддържа и допълнителни данни и метаданни за потребителите, но само такива, които не са включени като реквизити в централизирания профил на потребителя в Системата за електронна идентификация.

- Системата трябва да се съобразява с предпочитанията на потребителите, дефинирани в потребителските им профили в Системата за електронна идентификация, по отношение на предпочитаните комуникационни канали и канали за получаване на нотификации.

7.1.5. Отворени данни

- Трябва да бъде разработен и внедрен онлайн интерфейс за свободен публичен автоматизиран достъп до документите, информацията и данните в Системата (наричани заедно „данните"). Интерфейсът трябва да осигурява достъп до данните в машинночетим, отворен формат, съгласно всички изисквания на Директива 2013/37/ЕС за повторна употреба на информацията в обществения сектор и на Закона за достъп до обществена информация;
- Да бъде предвидена разработката и внедряването на отворени онлайн интерфейси и практически механизми, които да улеснят търсенето и достъпа до данни, които са на разположение за повторна употреба, като например списъци с основни документи и съответните метаданни, достъпни онлайн и в машинночетим формат, както и интеграция с Портала за отворени данни http://opendata.qovernment.bg, който съдържа връзки и метаданни за списъците с материали, съгласно изискванията на Закона за достъп до обществена информация (ЗДОИ);
- Трябва да се разработи и да се поддържа актуално публично описание на всички служебни и отворени интерфейси, отворените формати за данни, заедно с историята на промените в тях, в структуриран машинночетим формат;
- Трябва да се разработят процеси по предоставяне на данни в отворен, машинночетим формат заедно със съответните метаданни. Форматите и метаданните следва да съответстват на официалните отворени стандарти.

7.1.6. Формиране на изгледи

Потребителите на Системата трябва да получават разрези на информацията чрез филтриране, пренареждане и агрегиране на данните. Резултатът се представя чрез:

- Визуализиране на таблици;
- Графична визуализация на екран;
- Разпечатване на хартиен носител;
- Експорт на данни в един или в няколко от изброените формати - ODF, Excel, PDF, HTML, TXT, XML, CSV.

7.1.7. Администриране на Системата

Системата трябва да осигурява администриране на потребителите и правата за достъп.

7.2. Нефункционални изисквания към информационната система

Общи нефункционални изисквания към САИС:

- Да бъде централизирана, уеб базирана;
- Да работи с база данни;
- Да позволява многопотребителска работа;
- Да осигури интегритет при управлението на регистрите (използването на единни класификатори/списъци/номенклатури);
- Да поддържа история на данните и на техните промени;
- Да поддържа одитни записи;
- Дизайнът да позволява бъдещо разширение и подобрения, също така и съвместимост със съществуващи външни и вътрешни системи (с цел интегрирането им на следващи фази);
- Публичната част на системата да позволява работа с различни браузъри (Microsoft Internet Explorer, Mozilla, Firefox);
- Системата да извършва проверка на въвежданите от потребителите данни, като например формат, задължителност и др. Пълният набор проверки следва да се установи по време на етапите анализ и проектиране;
- Системата трябва да осигурява цялостност (интегритет) на данните при многопотребителски режим на работа;
- Системата трябва да осигурява непрекъсната 24/7 работоспособност;
- Да има възможност за архивиране и възстановяване както на нейната работоспособност така и на данните.

7.2.1. Авторски права и изходен код

- Всички компютърни програми, които се разработват за реализиране на Системата, трябва да отговарят на критериите и изискванията за софтуер с отворен код;
- Всички авторски и сродни права върху произведения, обект на закрила на Закона за авторското право и сродните му права, включително, но не само, компютърните програми, техният изходен програмен код, структурата и дизайнът на интерфейсите и базите данни, чието разработване е включено в предмета на поръчката, възникват за Възложителя в пълен обем без ограничения в използването, изменението и разпространението им и представляват произведения, създадени по поръчка на Възложителя съгласно чл. 42, ал. 1 от Закона за авторското право и сродните му права;
- Приложимите и допустими лицензи за софтуер с отворен код са:

  - GPL (General Public License) 3.0
  - LGPL (Lesser General Public License)
  - AGPL (Affero General Public License)
  - Apache License 2.0
  - New BSD license
  - MIT License **о** Mozilla Public License 2.0
- Изходният код (Source Code), разработван по проекта, както и цялата техническа документация трябва да бъде бъдат публично достъпни онлайн като софтуер с отворен код от първия ден на разработка чрез използване на система за контрол на версиите и хранилището по чл. 7в, т.18 от ЗЕУ;
- Да се изследва възможността резултатният продукт (Системата) да се изгради частично (библиотеки, пакети, модули) или изцяло на базата на съществуващи софтуерни решения, които са софтуер с отворен код. Когато е финансово оправдано, да се предпочита този подход пред изграждането на собствено софтуерно решение в цялост, от нулата. Избраният подход трябва да бъде детайлно описан в техническото предложение на участниците;
- Да бъде предвидено използването на Система за контрол на версиите и цялата информация за главното копие на хранилището, прието за оригинален и централен източник на съдържанието, да бъде достъпна публично, онлайн, в реално време.

7.2.2. Системна и приложна архитектура

- Системата трябва да бъде реализирана като разпределена модулна информационна система. Системата трябва да бъде реализирана със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки. Съществуващите модули функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящето изискване;
- Бизнес процесите и услугите трябва да бъдат проектирани колкото се може по-независимо с цел по-лесно надграждане, разширяване и обслужване. Системата трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс;
- Трябва да бъде реализирана функционалност за текущ мониторинг, анализ и контрол на изпълнението на бизнес процесите в Системата;
- При разработката, тестването и внедряването на Системата Изпълнителят трябва да прилага наложили се архитектурни (SOA, MVC или еквивалентни) модели и дизайн-шаблони, както и принципите на обектно ориентирания подход за разработка на софтуерни приложения;
- Системата трябва да бъде реализирана със софтуерна архитектура, ориентирана към услуги - Service Oriented Architecture (SOA);
- Взаимодействията между отделните модули в Системата и интеграциите с

външни информационни системи трябва да се реализират и опишат под формата на уеб-услуги (Web Services), които да са достъпни за ползване от други системи в държавната администрация, а за определени услуги - и за гражданите и бизнеса; За всеки от отделните модули/функционалности на Системата следва да се реализират и опишат приложни програмни интерфейси - Application Programming Interfaces (API). Приложните програмни интерфейси трябва да са достъпни и за интеграция на нови модули и други вътрешни или външни системи;

- Приложните програмни интерфейси и информационните обекти задължително да поддържат атрибут за версия;
- Версията на програмните интерфейси, представени чрез уеб-услуги, трябва да поддържа версията по един или няколко от следните начини:
    - Като част от URL-а
    - Като GET параметър
    - Като HTTP header (Accept или друг)
- За всеки отделен приложен програмен интерфейс трябва да бъде разработен софтуерен комплект за интеграция (SDK) на поне две от популярните развойни платформи (.NET, Java, PHP);
- Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля;
- При разработването на Системата трябва да се предвидят възможни промени, продиктувани от непрекъснато променящата се нормативна, бизнес и технологична среда. Основно изискване се явява необходимостта информационната система да бъде разработена като гъвкава и лесно адаптивна, като отчита законодателни, административни, структурни или организационни промени, водещи до промени в работните процеси;
- Изпълнителят трябва да осигури механизми за реализиране на бъдещи промени в Системата без промяна на съществуващия програмен код. Когато това не е възможно, времето за промяна, компилиране и пускане в експлоатация трябва да е сведено до минимум. Бъдещото развитие на Системата ще се налага във връзка с промени в правната рамка, промени в модела на работа на потребителите, промени във външни системи, интегрирани със Системата, отстраняване на констатирани проблеми, промени в модела на обслужване и др. Такива промени ще се извършват през целия период на експлоатация на Системата, включително и по време на гаранционния период;
- Архитектурата на Системата и всички софтуерни компоненти (системни и приложни) трябва да бъдат така подбрани и/или разработени, че да осигуряват работоспособност и отказоустойчивост на Системата, както и недискриминационно инсталиране (без различни условия за инсталиране върху физическа и виртуална среда) и опериране в продуктивен режим, върху виртуална инфраструктура, съответно върху Държавния хибриден частен облак

(ДХЧО);

- Изпълнителят трябва да проектира, подготви, инсталира и конфигурира като минимум следните среди за Системата: тестова, продуктивна;
- Системата трябва да бъде разгърната върху съответните среди (тестова за вътрешни нужди и продуктивна);
- Мрежата на държавната администрация (ЕЕСМ) ще бъде използвана като основна комуникационна среда и като основен доставчик на защитен Интернет капацитет (Clean Pipe) - изискванията на софтуерните компоненти по отношение на използвани комуникационни протоколи, TCP портове и пр. трябва да бъдат детайлно документирани от Изпълнителя, за да се осигури максимална защита от хакерски атаки и външни проникванията чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и ЕЕСМ;
- В Техническото си предложение участникът трябва да опише добрите практики, които ще прилага по отношение на всеки аспект от системната и приложната архитектура на Системата;
- За търсене трябва да се използват системи за пълнотекстово търсене (например Solr, Elastic Search). Не се допуска използването на индекси за пълнотекстово търсене в СУБД;
- Трябва да бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера;
- Всеки обект в системата трябва да има уникален идентификатор;
- Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис.

7.2.3. Повторно използване (преизползване) на ресурси и готови разработки

Проектът следва максимално да преизползва налични публично достъпни инструменти, библиотеки и платформи с отворен код.

За реализацията на Системата следва да се използват в максимална степен софтуерни библиотеки и продукти с отворен код.

Подход за избор на отворени имплементации и продукти

За реализацията на дадена техническа функционалност обикновено съществуват множество отворени алтернативни проекти, които могат да се използват в настоящата Система. Участникът следва да представи базов списък със свободните компоненти и средства, които възнамерява да използва. Отворените проекти трябва да отговарят на следните критерии:

- За разработката им да се използва система за управление на версиите на кода и да е наличен механизъм за съобщаване на несъответствия и приемане на допълнения;
- Да имат разработена техническа документация за актуалната стабилна версия;
- Да имат повече от един активен програмист, работещ по развитието им;
- Да имат възможност за предоставяне на комерсиална поддръжка;

- Да нямат намаляваща от година на година активност;
- По възможност проектите да са подкрепени от организации с идеална цел, държавни или комерсиални организации;
- По възможност проектите да имат разработени unit tests с code coverage над 50%, а проектът да използва Continuous Integration (CI) подходи - build bots, unit tests run, регулярно използване на статични/динамични анализатори на кода и др.

Препоръчително е преизползването на проекти, финансирани със средства на Европейския съюз, както и на такива, в които Участникът има активни разработчици. Използването на closed source и на инструменти, библиотеки, продукти и системи с платен лиценз става за сметка на Изпълнителя, като е допустимо в случаите, когато липсва подходяща свободна алтернатива с необходимата функционалност или тя не отговаря на горните условия.

Изпълнителят трябва да осигури поддръжка от комерсиална организация, развиваща основните отворени продукти, които ще бъдат използвани като минимум за операционните системи и софтуерните продукти за управление на базите данни.

Подход за работа с външните софтуерни ресурси

При използването на свободни имплементации на софтуерни библиотеки е необходимо да се организира копие (fork) на съответното хранилище в общото хранилище за проекти с отворен код, финансирани с публични средства в България (към момента https://github.com/governmentbg).

Използващите свободните библиотеки компоненти задават за "upstream repo" хранилищата в областта governmentbg, като задължително се реферира използваната версия/commit identificator.

Когато се налага промяна в изходния код на използван софтуерен компонент, промените трябва да се извършват във fork хранилището на governmentbg в съответствие с изискванията на основния проект. Изпълнителят трябва да извърши необходимите действия за включване на направените промени в основния проект чрез "pull requests" и извършване на необходимите изисквани от разработчиците на основния проект промени до приемането им. Тези дейности трябва да бъдат извършвани по време на целия проект.

При установяване на наличие на нови версии на използваните проекти се извършва анализ на влиянието върху настоящата система. В случаите, при които се оптимизира използвана функционалност, отстраняват се пропуски в сигурността, стабилността или бързодействието, новата версия се извлича и използва след успешното изпълнение на интеграционните тестове.

7.2.4. Изграждане и поддръжка на множество среди

Изпълнителят трябва да изгради и поддържа минимум следните логически разделени среди:

Среда	Описание
Development	чрез Development средата се осигурява работата по разработката,

	усъвършенстването и развитието на Системата. В тази среда са налични и допълнителните софтуерни системи и инсталации, необходими за управление на разработката – continuous integration средства, системи за автоматизирано тестване и др.
Testing	чрез Testing средата се извършват тестове, преди разгръщане на нова версия от Development средата върху Production средата. В нея се извършват всички интеграционни тестове, както и тестовете за натоварване. Всички, които трябва да се интегрират към Системата могат да тестват в нея интеграцията си, без да застрашават работата на продукционната среда.
Production	това е средата, която е публично достъпна за реална експлоатация и интеграция със съответните външни системи и услуги.

Управлението на средите трябва да става чрез автоматизирана система за провизиране и разгръщане на системните компоненти. При необходимост от страна на Възложителя Изпълнителят трябва да съдейства за изграждането на нови системни среди.

Участникът може да предложи изграждането на допълнителни среди според спецификите на предложеното решение.

7.2.5. Процес на разработка, тестване и разгръщане

Процесите, свързани с развитието на Системата, трябва да гарантират висока прозрачност и възможност за обществен контрол над всички разработки по проекта. Изграждането на доверие в гражданите и в бизнеса налага радикално по-висока публичност и прозрачност чрез отворена разработка и публикуването на системите компоненти под отворен лиценз от самото начало на разработката. По този начин гражданите биха могли да съдействат в процесите по развитие и тестване на разработките през целия им жизнен цикъл.

Всички софтуерни приложения, системи, подсистеми, библиотеки и компоненти, които са необходими за реализацията на Системата, трябва да бъдат разработвани като софтуер с отворен код и да бъдат достъпни в публично хранилище. Към настоящия момент следва да се използва общото хранилище за проекти с отворен код, финансирани с публични средства в България (към момента https://qithub.com/qovernmentbq).

В случай че върху част от компонентите, нужни за компилация, има авторски права, те могат да бъдат или в отделно хранилище с подходящия за това лиценз или за тях трябва да бъде предоставен заместващ „mock up“ компонент, така че да не се нарушава компилацията на проекта.

Трябва да се анализират възможностите за включване на граждани в процесите по разработка, тестване и идентифициране на пропуски на софтуера. Участникът трябва да предложи механизъм и процедури за реализирането на такива процеси. За всеки един разработван компонент Изпълнителят трябва да покрие следните изисквания за гарантиране на качеството на извършваната разработка и на крайния продукт:

- Документиране на Системата в изходния код, минимум на ниво процедура/функция/клас;
- Покритие на минимум 50% от изходния код с функционални тестове

- Използване на continuous integration практики;
- Използване на dependency management.

Участникът трябва да опише детайлно подхода си за покриване на изискванията.

Във всеки един компонент на Системата, който се build-ва и подготвя за инсталация (deployment), е необходимо да присъстват следните реквизити:

- Дата и час на build;
- Място/среда на build;
- Потребител извършил/стартирал build процеса;
- Идентификатор на ревизията от кодовото хранилище на компонента, срещу която се извършва build-ът.

7.2.7. Бързодействие и мащабируемост

Контрол на натоварването и защита от DoS/DDoS атаки

- Системата трябва да поддържа на приложно ниво "Rate Limiting" и/или "Throttling" на заявки от един и същ клиентски адрес както към страниците с уеб- съдържание, така и по отношение на заявките към приложните програмни интерфейси, достъпни публично или служебно като уеб-услуги (Web Services) и служебни интерфейси.
- Системата трябва да позволява конфигуриране от страна на администраторите на лимитите за отделни страници, уеб-услуги и ресурси, които се достъпват с отделен URL/URI.
- Системата трябва да поддържа възможност за конфигуриране на различни лимити за конкретни автентикирани потребители (напр. системи на други администрации) и трябва да предоставя възможност за генериране на справки и статистики за броя заявки по ресурси и услуги.

Кохерентно кеширане на данни и заявки

Не се изисква.

Бързодействие

- При визуализация на уеб-страници системите трябва да осигуряват висока производителност и минимално време за отговор на заявки - средното време за заявка трябва да бъде по-малко от 1 секунда, с максимум 1 секунда стандартно отклонение за 95% от заявките, без да се включва мрежовото времезакъснение (Network Latency) при транспорт на пакети между клиента и сървъра.
- Трябва да бъдат създадени тестове за натоварване.

Използване на HTTP/2

С оглед намаляване на служебния трафик, времената за отговор и натоварването на сървърите следва да се използва HTTP/2 протокол при предоставяне на публични потребителски интерфейси с включени като минимум следните възможности:

- Включена header compression;
- Използване на brotli алгоритъм за компресия;
- Включен HTTP pipelining;
- HTTP/2 Server push, приоритизиращ специфични компоненти, изграждащи страниците (CSS, JavaScript файлове и др.);
- Публичните потребителски интерфейси трябва да поддържат адаптивен избор на TLS cipher suites според вида на процесорната архитектура на клиентското устройство - AES-GCM за x86 работни станции и преносими компютри (с налични AES-NI CPU разширения), и ChaCha20/Poly1305 за мобилни устройства (основно базирани на ARM процесори);
- Ако клиентският браузър/клиент не поддържа HTTP/2, трябва да бъде предвиден fall-back механизъм към HTTP/1.1. Тази възможност трябва да може лесно да се реконфигурира в бъдеще и да отпадне, когато браузърите/клиентите, неподдържащи HTTP/2, станат незначителен процент.

Подписване на документи

Неприложимо.

Качество и сигурност на програмните продукти и приложенията

- Да бъде предвидено спазването на добри практики на софтуерната разработка - покритие на изходния код с тестове - над 60%, документиране на изходния код, използване на среда за непрекъсната интеграция (Continuous Integration), възможност за компилиране и пакетиране на продукта с една команда, възможност за инсталиране на нова версия на сървъра с една команда, система за управление на зависимостите (Dependency Management);
- Публичните модули, които ще предоставят информация и електронни услуги в Интернет, трябва да отговарят на актуалните уебстандарти за визуализиране на съдържание.

7.2.7. Информационна сигурност и интегритет на данните

- Не се допуска съхранението на пароли на администратори, на вътрешни и външни потребители и на акаунти за достъп на системи (ако такива се използват) в явен вид. Всички пароли трябва да бъдат защитени с подходящи сигурни алгоритми (напр. BCrypt, PBKDF2, scrypt (RFC 7914) за съхранение на пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption);
- Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата;
- Не се допуска използването на Self-Signed сертификати за публични услуги;
- Всички уебстраници (вътрешни и публично достъпни в Интернет) трябва да бъдат достъпни единствено и само през протокол HTTPS. Криптирането трябва

да се базира на сигурен сертификат с валидирана идентичност (Verified Identity), позволяващ задължително прилагане на TLS 1.2, който е издаден от удостоверителен орган, разпознаван от най-често използваните браузъри (Microsoft Internet Explorer, Google Chorme, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката;

- Трябва да бъдат извършени тестове за сигурност на всички уебстраници, като минимум чрез автоматизираните средства на SSL Labs за изпитване на сървърна сигурност (https://www.ssllabs.com/ssltest/). За нуждите на автентикация с КЕП трябва да се предвиди имплементирането на обратен прокси сървър (Reverse Proxy) с балансиране на натоварването, който да препраща клиентските сертификати към вътрешните приложни сървъри с нестандартно поле (дефинирано в процеса на разработка на Системата) в HTTP Header-a. Схемата за проксиране на заявките трябва да бъде защитена от Spoofing;
- Като временна мярка за съвместимост настройките на уебсървърите и Reverse Proxy сървърите трябва да бъдат балансирани така, че Системата да позволява използване и на клиентски браузъри, поддържащи по-стария протокол TLS 1.1. Това изключение от общите изисквания за информационна сигурност не се прилага за достъпа на служебни потребители от държавната администрация и доставчици на обществени услуги, които имат служебен достъп до ресурси на Системата;
- При разгръщането на всички уебуслуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2;
- Програмният код трябва да включва методи за автоматична санитизация на въвежданите данни и потребителски действия за защита от злонамерени атаки, като минимум SQL инжекции, XSS атаки и други познати методи за атаки, и да отговаря, където е необходимо, на Наредбата за оперативна съвместимост и информационна сигурност;
- При проектирането и разработката на компонентите на Системата и при подготовката и разгръщането на средите трябва да се спазват последните актуални препоръки на OWASP (Open Web Application Security Project);
- Трябва да бъде изграден модул за проследимост на действия и събития в Системата. За всяко действие (добавяне, изтриване, модификация, четене) трябва да съдържа следните атрибути:
    - Уникален номер;
    - Точно време на възникване на събитието;
    - Вид (номенклатура от идентификатори за вид събитие);
    - Данни за информационна система, където е възникнало събитието;
    - Име или идентификатор на компонент в информационната система, регистрирал събитието;
    - Приоритет;
    - Описание на събитието;

- Данни за събитието.

- Астрономическото време за удостоверяване настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута, секунда и при технологична необходимост – милисекунда, изписани в съответствие със стандарта БДС ISO 8601:2006;
- Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставимост, трябва да бъде удостоверявано с електронен времеви печат по смисъла на Глава III, Раздел 6 от Регламент ЕС 910/2014. Трябва да бъде реализирана функционалност за получаване на точно астрономическо време, отговарящо на горните условия, и от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161;
- Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата.

7.2.8. Използваемост

Общи изисквания за използваемост и достъпност

- При проектирането и разработката на софтуерните компоненти и потребителските интерфейси трябва да се спазват стандартите за достъпност на потребителския интерфейс за хора с увреждания WCAG 2.0, съответстващ на ISO/IEC 40500:2012;
- Всички ресурси трябва да са достъпни чрез GET заявка на уникален адрес (URL). Не се допуска използване на POST за достигане до формуляр за подаване не заявление, за генериране на справка и други;
- Функционалностите на потребителския интерфейс на Системата трябва да бъдат независими от използваните от потребителите интернет браузъри и устройства, при условие че последните са версии в период на поддръжка от съответните производители. Трябва да бъде осигурена възможност за ползване на публичните модули на приложимите услуги през мобилни устройства - таблети и смарт-телефони, чрез оптимизация на потребителските интерфейси за мобилни устройства (Responsive Design);
- Не се допуска използване на Капча (Captcha) като механизъм за ограничаване на достъпа до документи и/или услуги. Алтернативно, Системата трябва да поддържа "Rate Limiting" и/или "Throttling" съгласно изискванията в т. 7.1.1. от настоящите изисквания. Допуска се използването на Captcha единствено при иденетифицирани много последователни опити от предполагаем „бот“;
- Трябва да бъде осигурен бърз и лесен достъп до електронните услуги и те да бъдат промотирани с подходящи навигационни елементи на публичната интернет страница - банери, елементи от главното меню и др.;
- Публичните уеб страници на Системата трябва да бъдат проектирани и оптимизирани за ефективно и бързо индексиране от търсещи машини с цел популяризиране сред потребителите и по-добра откриваемост при търсене по ключови думи и фрази. При разработката на страниците и при изготвяне на

автоматизираните процедури за разгръщане на нова версия на Системата трябва да се използват инструменти за минимизиране и оптимизация на размера на изходния код (HTML, JavaScript и пр.) с оглед намаляване обема на файловете и по-бързо зареждане на страниците;

- Не се допуска използването на HTML Frames, за да не се пречи на оптимизациите за търсещи машини;
- При разработката на публични уеббазирани страници трябва да се използват и да се реализира поддръжка на:
    - Стандартните семантични елементи на HTML5 (HTML Semantic Elements);
    - JSON-LD 1.0 (http://www.w3.org/TR/ison-ld/);
    - Open Graph Protocol (http://ogp.me) за осигуряване на поддръжка за качествено споделяне на ресурси в социални мрежи и мобилни приложения;
- В екранните форми на Системата трябва да се използват потребителски бутони с унифициран размер и лесни за разбиране текстове в еднакъв стил.
- Всички текстови елементи от потребителския интерфейс трябва да бъдат визуализирани с шрифтове, които са подходящи за изобразяване на екран и които осигуряват максимална съвместимост и еднакво възпроизвеждане под различни клиентски операционни системи и браузъри. Не се допуска използването на серифни шрифтове (Serif).
- Полета, опции от менюта и командни бутони, които не са разрешени конкретно за ролята на влезлия в системата потребител, не трябва да са достъпни за този потребител. Това не отменя необходимостта от ограничаване на достъпа до бизнес логиката на приложението чрез декларативен или програмен подход.
- Всяка екранна форма трябва да има наименование, което да се изписва в горната част на екранната форма. Наименованията трябва да подсказват на потребителя какво е предназначението на формата.
- Всички търсения трябва да са нечувствителни към малки и главни букви.
- Полетата за пароли трябва задължително да различават малки и главни букви.
- Полетата за потребителски имена трябва да позволяват използване на имейл адреси като потребителско име, включително да допускат всички символи, регламентирани в RFC 1123, за наименуването на хостове;
- Главните и малките букви на въвежданите данни се запазват непроменени, не се допуска Системата да променя капитализацията на данните, въвеждани от потребителите.
- Системата трябва да позволява въвеждане на данни, съдържащи както български, така и символи на официалните езици на ЕС.
- Наименованията на полетата следва да са достатъчно описателни, като максимално се доближават до характера на съдържащите се в тях данни.
- Системата трябва да поддържа прекъсване на потребителски сесии при липса на активност. Времето трябва да може да се променя от администратора на системата без промяна в изходния код. Настройките за време за прекъсване на

неактивни сесии трябва да включват и възможността администраторите да дефинират стилизирана страница с информативно съобщение, към която Системата да пренасочва автоматично браузърите на потребителите в случай на прекъсната сесия;

- Дългите списъци с резултати трябва да се разделят на номерирани
- страници с подходящи навигационни елементи за преминаване към предишна, следваща, първа и последна страница, към конкретна страница.
- Навигационните елементи трябва да са логически обособени и свързани със съответния списък и да се визуализират в началото и в края на HTML контейнера, съдържащ списъка;
- За големите йерархически категоризации трябва да се предвиди възможност за навигация по нива или чрез отложено зареждане (lazy load).

Интернационализация

- Системата трябва да може да съхранява и едновременно да визуализира данни и съдържание, което е въведено/генерирано само на български език;
- Всички софтуерни компоненти на Системата, използваните софтуерни библиотеки и развойни комплекти, приложните сървъри и сървърите за управление на бази данни, елементите от потребителския интерфейс, програмно-приложните интерфейси, уебуслугите и др. трябва да поддържат стандартно и да са конфигурирани изрично за спазване на минимум Unicode 5.2 стандарт при съхранението и обработката на текстови данни, съответно трябва да се използва само UTF-8 кодиране на текстовите данни.
- Всички публично достъпни потребителски интерфейси следва да поддържат многоезичност, като минимум български и английски език.
- Публичната част на Системата трябва да бъде разработена и да включва набори с текстове на минимум два официални езика в ЕС, а именно български и английски език. Преводите на английски език трябва да бъдат осъществени професионално, като не се допуска използването на средства за машинен превод без ръчна проверка и корекции от професионални преводачи.
- Версиите на съдържанието на съответните езици трябва да включват всички текстове, които се визуализират във всички елементи на потребителския интерфейс, справките, генерираните от системата електронни документи, съобщения, нотификации, имейл съобщения, номенклатурите и таксономиите и др. Данните, които се съхраняват в Системата само на български език, се изписват/визуализират на български език;
- Публичната част на Системата трябва да позволява превключване между работните езици на потребителския интерфейс в реално време от профила на потребителя и от подходящ, видим и лесно достъпен навигационен елемент в горната част на всяка страница, който включва не само текст, но и подходяща интернационална икона за съответния език;
- При визуализация на числа трябва да се използва разделител за хиляди (интервал).

- При визуализация на дати и точно време в елементи от потребителския интерфейс в генерирани справки или в електронни документи всички формати за дата и час трябва да са съобразени с избрания от потребителя език/локация в настройките на неговия профил:
    - За България стандартният формат е „DD.MM.YYYY HH:MM:SS”, като наличието на време към датата е в зависимост от вида на визуализираната информация и бизнес-смисъла от показването на точно време;
    - Системата трябва да поддържа и всички формати съгласно ISO БДС 8601:2006;

Изисквания за използваемост на потребителския интерфейс

- Електронните форми за подаване на заявления и за обявяване на обстоятелства трябва да бъдат реализирани с AJAX или с аналогична технология, като по този начин се гарантират следните функционалности:
    - Контекстна валидация на въвежданите данни на ниво "поле" от форма и контекстни съобщения за грешка/невалидни данни в реално време;**o** Възможност за избор на стойности от номенклатури чрез търсене в списък по част от дума (autocomplete) и визуализиране на записи, отговарящи на въведеното до момента, без да е необходимо пълните номенклатури да са заредени в браузъра на клиента и потребителят да скролира дълги списъци с повече от 10 стойности;
- В електронните форми трябва да бъде реализирана валидация на въвежданите от потребителите данни на ниво "поле" (in-line validation). Валидацията трябва да се извършва в реално време на сървъра, като при успешна валидация данните от съответното поле следва да бъдат запазени от сървъра;
- Системата трябва да гарантира, че въведените, валидираните и запазените от сървъра данни остават достъпни за потребителите дори за процеси, които не са приключили, така че при волно, неволно или автоматично прекъсване на потребителската сесия поради изтичане на периода за допустима липса на активност потребителят да може да продължи съответния процес след повторно влизане в системата, без да загуби въведените до момента данни и прикачените до момента електронни документи;
- Трябва да бъде реализирана възможност за добавяне и редактиране от страна на администраторите на Системата, без да са необходими промени в изходния код, на контекстна помощна информация за:
    - всяка електронна форма или стъпка от процес, за която има отделен екран/форма;
    - всяка група полета за въвеждане на данни (в случаите, в които определени полета от формата са групирани тематично);
    - всяко отделно поле за въвеждане на данни;
- Трябва да бъде разработена контекстна помощна информация за всички процеси, екрани и електронни форми, включително ясни указания за попълване и разяснения за особеностите при попълване на различните групи полета или на

отделни полета;

- Контекстната помощна информация, указанията към потребителите и информативните текстове за всяка електронна административна услуга не трябва да съдържат акроними, имена и референции към нормативни документи, които са въведени като обикновен текст (plain-text). Всички акроними, референции към нормативни документи, формуляри, изисквания и др. трябва да бъдат разработени като хипервръзки към съответните актуални версии на нормативни документи и/или към съответния речник/списък с акроними и термини;
- Достъпът на потребителя до контекстната помощна информация трябва да бъде реализиран по унифициран и консистентен начин чрез подходящи навигационни елементи, като например чрез подходящо разположени микро-бутони с икони, разположени до/пред/след етикета на съответния елемент, за който се отнася контекстната помощ, или чрез обработка на "Mouse Hover/Mouse Over" събития;
- При проектирането и реализацията на потребителския интерфейс трябва да се отчете, че той трябва да бъде еднакво използваем и от мобилни устройства (напр. таблети), които не разполагат с мишка, но имат чувствителни на допир екрани.
- Потребителският интерфейс следва да бъде достъпен за хора с увреждания съгласно изискванията на чл. 48, ал. 5 от ЗОП.

Изисквания за използваемост в случаи на прекъснати бизнес процеси

- Системата трябва да съхранява перманентно всеки започнал процес/процедура по подаване на заявление или обявяване на обстоятелства, текущия му статус и всички въведени данни и прикачени документи дори ако потребителят е прекъснал волно или неволно потребителската си сесия;
- При вход в системата потребителят трябва да получава прегледна и ясна нотификация, че има започнати, но недовършени/неизпратени/неподписани заявления, и да бъде подканен да отвори модула за преглед на историята на транзакциите;
- Модулът за преглед на историята на транзакциите трябва да поддържа следните функционалности:
    - Да визуализира списък с историята на подадените заявления, като минимум със следните колони - дата, входящ номер, код на тупа формуляр, подател (име на потребител и имена на физическото лице - подател), статус на заявлението;
    - Да предлага видни и лесни за използване от потребителите контроли/инструменти:
    - за филтриране на списъка (от дата до дата, за предефинирани периоди, като "последния един месец", "последната една година";
    - сортиране на списъка по всяка от колоните, без това да премахва текущия филтър;

- свободно търсене по ключови думи по всички колони в списъка и метаданните на прикачените/свързаните документи със заявленията, което да води до динамично филтриране на списъка.

Изисквания за проактивно информиране на потребителите

Неприложимо.

7.2.9. Системен журнал

Изграждането решение задължително трябва да осигурява проследимост на действията на всеки потребител (одит), както и версия на предишното състояние на данните, които той е променил в резултат на своите действия (системен журнал).

Атрибутите, които трябва да се запазват при всеки запис, трябва да включват като минимум следните данни:

- дата/час на действието;
- модул на системата, в който се извършва действието;
- действие;
- обект, над който е извършено действието;
- допълнителна информация;
- IP адрес и браузър на потребителя.

Размерът на журнала на потребителските действия нараства по време на работа на всяка система, което налага по-различното му третиране от гледна точка на организация на базата данни:

- по време на работа на Системата потребителският журнал трябва да се записва в специализиран компонент, който поддържа много бързо добавяне на записи; този подход се налага, за да не се забавя излишно работата на Системата;
- специална фонова задача трябва да акумулира записаните данни и да ги организира в отделна специално предвидена за целта база данни, отделна от работната база данни на Системата;
- данните в специализираната база данни трябва да се архивират и изчистват, като в специализираната база данни трябва да бъде достъпна информация за не повече от 2 месеца назад; при необходимост от информация за предишен период администраторът на Системата трябва първо да възстанови архивните данни;
- трябва да бъде предоставен достъп до системния журнал на органите на реда чрез потребителски или програмен интерфейс; за достъпа трябва да се изисква електронна идентификация.

7.2.10. Дизайн на бази данни и взаимодействие с тях

При използване на база данни (релационна или нерелационна^оБОЬ) следва да бъдат следвани добрите практики за дизайн и взаимоедйствие с базата данни, в т.ч.:

- дизайнът на схемата на базата данни (ако има такава) трябва да бъде с

максимално ниво на нормализация, освен ако това не би навредило сериозно на производителността;

- базата данни трябва да може да оперира в клъстър; в определени случаи следва да бъде използван т.нар. sharding;
- имената на таблиците и колоните трябва да следват унифицирана конвенция;
- трябва да бъдат създадени индекси по определени колони, така че да се оптимизират най-често използваните заявки; създаването на индекс трябва да е мотивирано и подкрепено със замервания;
- връзките между таблици трябва да са дефинирани чрез foreign key;
- периодично трябва да бъде правен анализ на заявките, включително чрез EXPLAIN (при SQL бази данни), и да бъдат предприети мерки за оптимизиране на бавните такива;
- задължително трябва да се използват транзакции, като нивото на изолация трябва да бъде мотивирано в предадената документация;
- при операции върху много записи (batch) следва да се избягват дългопродължаващи транзакции;
- заявките трябва да бъдат ограничени в броя записи, които връщат;
- при използване на ORM или на друг слой на абстракция между приложението и базата данни, трябва да се минимизира броят на излишните заявки (т.нар. n+1 selects проблем);
- при използване на нерелационна база данни трябва да се използват по- бързи и компактни протоколи за комуникация, ако такива са достъпни.

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

8.1. Анализ и проектиране на Специализирана автоматизирана информационна система за поддържане на регистрите в КЗЛД, в изпълнение изискванията на новата правна рамка

8.1.1. Описание на дейността

На този етап Изпълнителят трябва да извърши анализ на новата правна рамка, свързана с поддържаните от КЗЛД регистри и да анализира нуждите на потребителите на регистрите.

8.1.2. Изисквания към изпълнение на дейността

Изпълнителят трябва да приложи световно утвърдена методология за извършване на анализ и изготвяне на Системен проект.

8.1.3. Очаквани резултати

- Аналитичен доклад с описание на детайлната спецификация към регистрите;
- Системен проект.

8.2. Разработка на софтуер

8.2.1. Описание на дейността

При изпълнението на дейността трябва да бъде разработено уеб базирано софтуерно решение за поддръжка на:

- Регистър на длъжностните лица по защита на данните;
- Регистър на акредитирани сертифициращи организации;
- Регистър на кодекси за поведение;
- Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия (Регистър на нарушенията и предприетите мерки).

8.2.2. Изисквания към изпълнение на дейността

Изпълнителят трябва да приложи световно утвърдена методология за извършване на софтуерна разработка, осигуряване на качество и изготвяне на потребителска и системна документация.

8.2.3. Очаквани резултати

- Разработен Регистър на длъжностните лица по защита на данните;
- Разработен Регистър на акредитирани сертифициращи организации;
- Разработен Регистър на кодекси за поведение;
- Разработен Регистър на нарушения на Регламент 2016/679 и на закона, както и на предприетите мерки в съответствие с упражняването на корективните правомощия (Регистър на нарушенията и предприетите мерки).
- Изготвена потребителска документация,
- Изготвена системна документация.
- Протокол от проведени тестове на софтуерната разработка.

8.3. Внедряване на системата и преминаване към редовна експлоатация

8.3.1. Описание на дейността

На този етап Изпълнителят трябва да инсталира разработения софтуер на сървъри на Възложителя. Изпълнителят трябва да извърши параметризация и конфигурация на системата.

Ако е необходимо, трябва да бъдат мигрирани съществуващи данни.

Изпълнителят трябва да обучи администратори и потребители на системата.

Изпълнителят, съвместно с Възложителя трябва да проведат тестове за потребителско приемане на системата.

8.3.2. Изисквания към изпълнение на дейността

Изпълнителят трябва да приложи добрите практики за разгръщане на системата върху инфраструктурата на Възложителя.

При наличие на съществуващи данни, Изпълнителят трябва да извърши тяхната миграция, като запази целостта и консистентността на данните.

За провеждане на обученията Изпълнителят трябва да осигури Ръководство на потребителя, Ръководство на администратора, обучителни материали, квалифицирани лектори.

8.3.3. Очаквани резултати

- Внедрена система за обслужване на 4 бр. регистри;
- Мигрирани данни при наличие на такива;
- Обучени администратори на системата – 2 бр.;
- Обучени потребители за работа със системата – 10 бр.;
- Проведени потребителски тестове без наличие на забележки.

9. ДОКУМЕНТАЦИЯ

9.1. Изисквания към документацията

- Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително и на нейните съставни части, трябва да бъдат налични и на български език;
- Всички документи трябва да бъдат предоставени от Изпълнителя в електронен формат (ODF/ /Office Open XML/MS Word DOC/RTF/PDF/HTML или др.), позволяващ пълнотекстово търсене/търсене по ключови думи и копиране на части от съдържанието от оригиналните документи във външни документи, за вътрешна употреба на възложителя;
- Навсякъде, където в документацията има включени диаграми или графики, те трябва да бъдат вградени в документите в оригиналния си векторен формат;
- Детайлна техническа документация на програмния приложен интерфейс (API), включително за поддържаните уебуслуги, команди, структури от данни и др. Документацията да бъде придружена и с примерен програмен код и/или библиотеки (SDK) за реализиране на интеграция с външни системи, разработен(и) на Java или .NET. Примерният код трябва да е напълно работоспособен и да демонстрира базови итерации с API-то:
    - Регистриране на крайна точка (end-point) за получаване на актуализации от Системата в реално време;
    - Заявки за получаване на номенклатурни данни (списъци, таксономии);
    - Заявки за актуализиране на номенклатурни данни (списъци, таксономии);
    - Регистрация на потребител;
    - Идентификация и оторизация на потребител или уебуслуга;
- Документацията за приложния програмен интерфейс (API) трябва да бъде публично достъпна;
- Всеки предоставен REST приложно-програмен интерфейс трябва да бъде документиран чрез API Blueprint (https://github.com/apiaryio/api-blueprint),

Swagger (http://swagger.io) или чрез аналогична технология. Аналогично представяне трябва да бъде изготвено и за SOAP интерфейсите;

- Детайлна техническа документация за схемата на базата данни - структури за данни, индекси, дялове, съхранени процедури, конфигурации за репликация на данни и др.
- Ръководства на потребителя и администратора за работа и администриране на Системата
- Обща информация, инструкции и процедури за администриране и поддръжка на приложните сървъри, сървърите за бази данни и др.
- Обща информация, инструкции и процедури за администриране, архивиране и възстановяване, и поддръжка на сървъра за управление на бази данни.

9.2. Прозрачност и отчетност

- В обхвата на проекта е включено извършване на дейности по анализ на бизнес процеси и нормативна уредба, проектиране на системна и приложна архитектура, разработване на компютърни програми и други дейности, свързани с предоставяне на специализирани професионални услуги. Изпълнителят и Възложителят трябва да публикуват подробни месечни отчети в машинночетим отворен формат за извършените дейности, включително количеството изработени човекодни по дейности, извършени от консултанти, експерти, специалисти и служители на Изпълнителя и Възложителя.

Документацията, предоставена от Изпълнителя на Възложителя, трябва да бъде:

- на български език;
- на хартия и в електронен формат; копирането и редактирането на предоставените документи следва да бъде лесно осъществимо;
- актуализирана в съответствие със съгласувана с възложителя процедура, която следва да включва документи, подлежащи на промяна/актуализация, крайни срокове и нужната за случая методология.

Минимално изискуемата документация по проекта включва долуизброените документи.

9.3. Системен проект

Изпълнителят на настоящата поръчка трябва да дефинира в детайли конкретния обхват на реализация на софтуерната разработка и да документира изискванията към софтуера в детайлна техническа спецификация (системен проект), която ще послужи за пряка изходна база за разработка.

При документирането на изискванията, с цел постигане на яснота и стандартизация на документите, е необходимо да се използва утвърдена нотация за описание на бизнес модели. Изготвената детайлна техническа спецификация (системен проект) се представя за одобрение на Възложителя. В случай на забележки, корекции или допълнения от страна на

Възложителя Изпълнителят е длъжен да ги отрази в детайлната техническа спецификация (системен проект).

9.4. Техническа документация

Всички продукти, които ще се доставят, трябва да са със специфична документация за инсталиране и/или техническа документация, в това число:

- Ръководство за администратора, включващо всички необходими процедури и скриптове по инсталиране, конфигуриране, архивиране, възстановяване и други, необходими за администриране на Системата;
- Документи за крайния ползвател - Изпълнителят трябва да предостави главното Ръководство на ползвателите на софтуера. Документът е предназначен за крайните ползватели. Той трябва да описва цялостната функционалност на приложния софтуер и съответното му използване от крайни ползватели;
- Детайлно описание на базата данни;
- Описание на софтуерните модули;
- Описание на изходния програмен код.

9.5. Протоколи

Изпълнителят трябва да изготвя протоколи от изпълнението на различните етапи на проекта, описани в раздел 8 на настоящия документ, заедно със съпътстващите ги документи - резултати от изпълнението на етапите.

9.6. Комуникация и доклади

За успешното изпълнение на проекта участниците в настоящата обществена поръчка трябва да предложат адекватен механизъм за управление на проектната комуникация, който е неразделна част от предлаганата цялостна проектна методология.

Управлението на комуникацията трябва да включва изготвяне на минимум следните регулярни доклади за статуса и напредъка на изпълнението на поръчката:

9.6.1. Встъпителен доклад

Встъпителният доклад трябва да бъде предоставен до един месец от подписването на договора и да съдържа описание минимум на:

- Подробен работен план и актуализиран времеви график за периода на проекта;
- Начини на комуникация;
- Отговорни лица и екипи.

Встъпителният доклад следва да бъде одобрен от Възложителя.

9.6.2. Междинни доклади

Междинните доклади трябва да бъдат представяни и да се предават при приключване на всяка от дейностите и поддейностите и/или при настъпване на събитие.

Междинните доклади трябва да съдържат информация относно изпълнението на дейностите и поддейностите по предварително изготвения проектен план.

Докладът за междинния напредък трябва да бъде подготвен по следния начин:

- Общ прогрес по дейностите през периода;
- Постигнати проектни резултати за периода;
- Срещнати проблеми, причини и мерки, предприети за преодоляването им;
- Рискове за изпълнение на свързани дейности и на проекта като цяло и предприети мерки;
- Актуализиран план за изпълнение, ако има такъв.
- Всеки междинен доклад следва да бъде одобрен от Възложителя.

9.6.3. Окончателен доклад

В края на периода за изпълнение трябва да се представи окончателен доклад. Окончателният доклад трябва да съдържа описание на изпълнението и резултати.

Докладите се изпращат до отговорния служител на Възложителя. За тази цел Възложителят ще определи в договора отговорния/отговорните служител/служители. Всички доклади се представят на български език в електронен формат и на хартиен носител. Докладите се одобряват от отговорния/отговорните служител/служители в срок до 5 (пет) работни дни.

Всички доклади трябва да се представят на възложителя на български език на хартиен и на електронен носител. Представянето на докладите трябва да се извършва чрез подписване на двустранни предавателно-приемателни протоколи, подписани от представители на Изпълнителя и на Възложителя.

Възложителят разглежда представените доклади и уведомява Изпълнителя за приемането им без забележки или ги връща за преработване, допълване и/или окомплектоване, ако не отговарят на изискванията, като чрез упълномощено в договора лице дава указания и определя срок за отстраняване на констатираните недостатъци и пропуски.

10. РЕЗУЛТАТИ

Очакваните резултати от изпълнението на настоящата обществена поръчка са следните:

(Описват се конкретните резултати съобразно одобреното проектно предложение)