

НАРЕДБА ЗА ОБЩИТЕ ИЗИСКВАНИЯ КЪМ ИНФОРМАЦИОННИТЕ СИСТЕМИ, РЕГИСТРИТЕ И ЕЛЕКТРОННИТЕ АДМИНИСТРАТИВНИ УСЛУГИ

Приета с ПМС № 3 от 9.01.2017 г., обн., ДВ, бр. 5 от 17.01.2017 г., в сила от 1.03.2017 г., изм. и доп., бр. 66 от 10.08.2018 г., в сила от 10.08.2018 г., бр. 4 от 14.01.2020 г., в сила от 14.01.2020 г., изм., бр. 47 от 24.06.2022 г., в сила от 24.06.2022 г., изм. и доп., бр. 80 от 20.09.2024 г.

Глава първа ОБЩИ ПОЛОЖЕНИЯ

Обхват

Чл. 1. (1) С наредбата се определят:

1. (нова – ДВ, бр. 80 от 2024 г.) изискванията за идентификация на длъжностни лица и информационни системи за нуждите на служебното предоставяне и изпращане на данните от първичните администратори на данни – по чл. 3, ал. 3 от ЗЕУ;
2. (нова – ДВ, бр. 80 от 2024 г.) други средства за електронна идентификация – по чл. 5, ал. 2, т. 4 от ЗЕУ;
3. (предишна т. 1 – ДВ, бр. 80 от 2024 г.) стандартът за единно време – по чл. 6 от Закона за електронното управление (ЗЕУ);
4. (предишна т. 2 – ДВ, бр. 80 от 2024 г.) условията и редът за представянето на информацията за съгласуване в рамките на бюджетния процес – по чл. 7г, ал. 6 ЗЕУ;
5. (нова – ДВ, бр. 80 от 2024 г.) редът за извеждане от експлоатация на информационните системи на административните органи – по чл. 7г, ал. 8 от ЗЕУ;
6. (предишна т. 3 – ДВ, бр. 80 от 2024 г.) редът за водене на регистрите на проектите и дейностите и на информационните ресурси – по чл. 7д и 7е ЗЕУ;
7. (предишна т. 4 – ДВ, бр. 80 от 2024 г.) допълнителните набори от данните за публикуване – по чл. 7п ЗЕУ;
8. (предишна т. 5 – ДВ, бр. 80 от 2024 г.) общите изисквания за предоставяне на електронни административни услуги – по чл. 12, ал. 4 ЗЕУ;
9. (предишна т. 6 – ДВ, бр. 80 от 2024 г.) начините за електронни разплащания по предоставянето на електронни административни услуги – по чл. 12, ал. 5 ЗЕУ;
10. (предишна т. 7 – ДВ, бр. 80 от 2024 г.) техническите изисквания за осигуряване на достъп до електронните административни услуги и политиките на доставчиците на електронни административни услуги за използваните графични и други интерфейси на информационните системи – по чл. 17, ал. 1 ЗЕУ;
11. (нова – ДВ, бр. 80 от 2024 г.) стандартите и редът за използване от административните органи на споделените ресурси на електронното управление – по чл. 17, ал. 4 от ЗЕУ;
12. (предишна т. 8 – ДВ, бр. 80 от 2024 г.) допълнителните начини за подаване на електронни документи и изявления от граждани и организации – по чл. 20, т. 3 и чл. 36, ал. 2 ЗЕУ;
13. (предишна т. 9 – ДВ, бр. 80 от 2024 г.) форматите и задължителните реквизити, на които трябва да отговарят електронните документи – по чл. 21 ЗЕУ;
14. (предишна т. 10 – ДВ, бр. 80 от 2024 г.) методите за установяване на интегритета и авторството на електронните изявления – по чл. 22, ал. 4 ЗЕУ;
15. (предишна т. 11 – ДВ, бр. 80 от 2024 г.) дейността на посредниците при електронни административни услуги – по чл. 24а ЗЕУ;
16. (*) (предишна т. 12 – ДВ, бр. 80 от 2024 г.) изискванията за електронен адрес за получаване на електронна административна услуга – по чл. 26 ЗЕУ;

16. (нова – ДВ, бр. 80 от 2024 г.) правилата за провеждане на одит на информационна система за сигурно електронно връчване, поддържана от Министерството на електронното управление – по чл. 26а, ал. 2 от ЗЕУ;
 17. (нова – ДВ, бр. 80 от 2024 г.) форматът на електронните адреси в системата за сигурно електронно връчване, поддържана от Министерството на електронното управление – по чл. 26а, ал. 4 от ЗЕУ;
 18. (предишна т. 13 – ДВ, бр. 80 от 2024 г.) случаите, в които електронно изявление се смята за получено от доставчика на електронни административни услуги – по чл. 32 ЗЕУ;
 19. (предишна т. 14 – ДВ, бр. 80 от 2024 г.) начините за потвърждаване на получаването на електронно изявление – по чл. 34, ал. 4 ЗЕУ;
 20. (предишна т. 15 – ДВ, бр. 80 от 2024 г.) редът за съхраняването на електронни документи – по чл. 38, ал. 2 ЗЕУ;
 21. (предишна т. 16 – ДВ, бр. 80 от 2024 г.) условията за автоматизиран обмен на електронни документи като вътрешни електронни административни услуги – по чл. 41 ЗЕУ;
 22. (предишна т. 17 – ДВ, бр. 80 от 2024 г.) редът за водене на регистъра на стандартите – по чл. 47 ЗЕУ;
 23. (предишна т. 18 – ДВ, бр. 80 от 2024 г.) редът за водене на регистъра на информационните обекти и стандартът за тяхното описание – по чл. 48 ЗЕУ;
 24. (предишна т. 19 – ДВ, бр. 80 от 2024 г.) редът на вписване на информационните обекти – по чл. 49 ЗЕУ;
 25. (нова – ДВ, бр. 80 от 2024 г.) редът за заявяване и използване на регистър чрез информационната система за централизирано изграждане и поддържане на регистри – по чл. 52а, ал. 4 от ЗЕУ;
 26. (нова – ДВ, бр. 80 от 2024 г.) стандартът, съгласно който се генерира уникален идентификатор на всеки запис в регистър – по чл. 52б, ал. 1, т. 3 от ЗЕУ;
 27. (нова – ДВ, бр. 80 от 2024 г.) общите изисквания към регистрите, включително за тяхното структуриране, функционалности и удостоверяване на данни – по чл. 52б, ал. 2 от ЗЕУ;
 28. (нова – ДВ, бр. 80 от 2024 г.) изискванията за информационна сигурност на регистрите, водени от административните органи и лицата по чл. 1, ал. 2 – по чл. 52б, ал. 3 от ЗЕУ;
 29. (предишна т. 20 – ДВ, бр. 80 от 2024 г.) редът за периодично създаване на резервни копия и архивиране на данните – по чл. 58а, т. 8 ЗЕУ;
 30. (предишна т. 21 – ДВ, бр. 80 от 2024 г.) специфични изисквания към информационните системи – по чл. 58а, т. 10 ЗЕУ.
- (2) (Изм. – ДВ, бр. 80 от 2024 г.) Наредбата се прилага по отношение на дейността по предоставянето на електронни административни услуги и на информационните системи на административните органи, доколкото в закон не е предвидено друго.

(*) *Бел. ред.* С § 1, т. 1, б. "е" на ПМС № 311 от 11.09.2024 г. за изменение и допълнение на Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (ДВ, бр. 80 от 2024 г.) в чл. 1, ал. 1 се преномерират точки, като досегашните т. 8, 9, 10, 11 и 12 стават съответно т. 12, 13, 14 и 15, но законодателят е изпуснал да даде преномерация на досегашната т. 12, която следва да се преномерираща на т. 16, поради което има две точки с номер 16.

Глава втора РЕГИСТРИ, ОПЕРАТИВНА СЪВМЕСТИМОСТ И ОБМЕН НА ДАННИ

Раздел I Регистри за оперативна съвместимост

Регистър на регистрите

Чл. 2. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление води регистър на регистрите, в който се вписват регистри и бази данни на първичните администратори на данни, в които се съдържат първични данни.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Заявлението за вписването в регистъра на регистрите се подава автоматично по електронен път от съответната информационна система от първичен администратор на данни, след като бъде идентифициран по реда на тази глава. Вписването се извършва от длъжностни лица, определени от министъра на електронното управление.

(3) Заявлението може да се подаде чрез потребителски интерфейс, когато информационната система не поддържа автоматично подаване на обстоятелства за вписване.

(4) В заявлението заявителят посочва URL на регистъра или базата данни, наименованието му, правното основание за водене на регистъра или базата данни и уникален идентификатор на първичния администратор.

Регистър на информационните обекти

Чл. 3. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление води регистъра на информационните обекти като част от Интегрираната информационна система на държавната администрация (ИИСДА).

(2) Първичните администратори на данни вписват автоматично в регистъра по ал. 1 формализирани описания на данните, на които са първичен администратор. Вписването се извършва чрез информационните системи на първичните администратори на данни.

(3) Регистърът съдържа формализирани описания на данни във формат XSD или JSON Schema.

(4) В регистъра се поддържат версии на информационните обекти.

(5) Информационните обекти могат да представляват структури от данни или номенклатури.

(6) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление дава методически указания и издава задължителни разпореждания на първичните администратори на данни относно вписването на информационни обекти по ал. 1.

Регистър на стандартите

Чл. 4. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Регистърът на стандартите е информативен списък с базови стандарти, на които трябва да отговарят информационните системи в държавната администрация, и се води от министъра на електронното управление.

(2) За всеки вписан стандарт се поддържа най-малко стандартизираща организация, ако има такава, и номер на стандарт.

(3) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Длъжностни лица, определени от министъра на електронното управление, осъвременяват стандартите, вписани в регистъра, поне веднъж на 6 месеца.

(4) За всеки стандарт в регистъра се поддържа статус:

1. Препоръчителен – административните органи могат да използват съответния стандарт.

2. Задължителен – административните органи са длъжни да използват съответния стандарт в определените в регистъра случаи.

(5) Когато стандарт се реферира в нормативен акт, в регистъра на стандартите се вписва конкретният нормативен текст със съответните приложими стандарти и техните версии.

Раздел II

Общи изисквания към регистрите и базите данни

Общи положения

Чл. 5. (1) (Изм. – ДВ, бр. 80 от 2024 г.) Изискванията в този раздел се отнасят за техническата реализация на регистрите и базите данни, водени от административните органи, когато това им е възложено със закон.

(2) (Отм. – ДВ, бр. 80 от 2024 г.).

(3) Изискванията не се отнасят и за бази данни, които не са свързани с предоставянето на административни услуги.

Идентификация на регистрите и базите данни

Чл. 6. (1) Регистър и база данни се идентифицират чрез електронно удостоверение във формат X.509, издаден за съответния регистър.

(2) Идентификацията се осъществява двустранно по протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2 или по-висока, дефиниран в Препоръка RFC 5246, приета от IETF (The Internet Engineering Task Force – Целева група за Интернет инженеринг) през август 2008 г.

(3) Идентификацията се осъществява с всяка информационна система, с която регистърът или базата данни извършва комуникация, включително регистъра на регистрите.

Достъп до регистрите и базите данни

Чл. 7. (1) Достъпът до регистрите и базите данни е свободен и безплатен, освен ако ограничение за това не произтича от закон.

(2) Лицата имат право на достъп по електронен път до всички данни в регистрите и базите данни, отнасящи се до тях, след като се идентифицират по ред, определен в закон, освен ако ограничение за това не произтича от закон.

(3) Административните органи предоставят програмни интерфейси за достъп до регистрите и базите данни.

(4) Достъпът до регистрите и базите данни се извършва:

1. по интернет – за публичния достъп и за служебния достъп от лица, които не са административни органи;

2. чрез Единната електронна съобщителна мрежа на държавната администрация или виртуална частна мрежа за административни органи или при обективна технологична необходимост.

(5) (Доп. – ДВ, бр. 80 от 2024 г.) Данните за физическите лица от регистрите са достъпни за центровете за електронна идентификация по Закона за електронна идентификация (ЗЕИ), както и за лицата, предоставящи услуга за електронна идентификация, посочена в чл. 5, ал. 2, т. 3 от Закона за електронното управление.

(6) Когато за достъп до регистър се изисква регистрация, лицата, включително чрез техни информационни системи, се идентифицират пред него по реда на тази глава.

(7) Достъпът до регистрите се извършва по следните начини:

1. синхронно с изпращане на заявка за предоставяне на резултат в реално време (модел "sync pull");

2. асинхронно с изпращане на заявка за предоставяне на резултат в по-късен момент (модел "async pull");
3. чрез служебно уведомяване до предварително регистрирана крайна точка (модел "subscribe – push").
- (8) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Достъпът до регистрите може да се извършва директно или чрез централен компонент, който гарантира спазването на изискванията на тази глава и отговаря на изисквания, определени от министъра на електронното управление. Централният компонент, включително правата за достъп до ресурси чрез него, се управлява от министъра на електронното управление.
- (9) Централният компонент задължително се поддържа в тестови режим, както и в режим за експериментална интеграция.
- (10) За всеки достъп до регистрите се записва време, удостоверявано чрез електронни времеви печати по глава III, раздел 6 от Регламент (ЕС) № 910/2014 на Европейския парламент и на съвета от 23 юли 2014 г. относно електронната идентификация и удостоверявателните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ, L 257 от 28 август 2014 г.) (Регламент № (ЕС) 910/2014).
- (11) Документация на интерфейсите по ал. 3, както и софтуерни библиотеки за достъп се предоставят публично, включително на портала за разработчици по чл. 61.
- (12) Достъпът до регистрите от административни органи се извършва като вътрешна административна услуга.

Условия за достъп

- Чл. 8. (1) Длъжностните лица, осъществяващи достъп до регистри и бази данни, използват данните само във връзка с осъществяване на правомощия, възложени на съответния административен орган или в други случаи, предвидени в закон.
- (2) Достъпът до регистрите и базите данни се осъществява чрез подаване на заявление, съдържащо минимум данни за:
1. произхода на заявлението – юридическото лице – заявител и информационната система;
 2. основанията за получаването на данните, включително номер на преписка, ако има такава;
 3. длъжностното лице, извършващо заявяването, ако има такова.
- (3) Първичен администратор на данни отказва достъп до данни на лицата, които ги заявяват, когато в заявлението за достъп по ал. 2 липсва един или повече от изискуемите реквизити или заявителят няма право да получи данните съгласно закон.
- (4) Заявлението по ал. 2, отговорът с поисканите данни и отказ по ал. 3 са само в електронна форма.
- (5) Процесите по обмен на данни по ал. 4 са автоматизирани, а когато няма технологична възможност за автоматизиран обмен между информационните системи, се допуска ръчен обмен по електронен път чрез потребителски интерфейс.
- (6) Първичен администратор може да използва автоматизирани методи за ограничаване на количеството заявки за достъп до регистър за определени периоди, когато големият брой заявки би нарушил нормалното му функциониране.
- (7) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) При системни нарушения на изискванията за обмен от страна на администрации, използващи достъп до данни от регистър, съответният първичен администратор има право временно да преустанови правото на достъп след съгласуване с министъра на електронното управление.

Удостоверителни административни услуги

Чл. 9. (1) Административните органи предоставят всички удостоверителни административни услуги и като електронни административни услуги чрез програмни интерфейси в съответствие с изискванията на тази наредба.

(2) Резултатът от предоставена по реда на ал. 1 електронна административна услуга има официална удостоверителна сила.

(3) Резултатът по ал. 1 се подписва електронно от съответния първичен администратор на данни, а времето на издаването му се удостоверява чрез електронен времеви печат по глава III, раздел 6 от Регламент № (ЕС) 910/2014.

(4) Ръководителите на администрациите или упълномощени от тях лица вписват услугите по ал. 1 и като вътрешни електронни административни услуги в административния регистър по чл. 61 от Закона за администрацията.

Идентификация пред регистър или база данни

Чл. 10. (1) Информационните системи на административните органи, на доставчиците на обществени услуги и на лицата, осъществяващи публични функции, се идентифицират пред регистрите чрез цифров сертификат, вписан в ИИСДА, двустранно по протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2 или по-висока, дефиниран в Препоръка RFC 5246, приета от IETF (The Internet Engineering Task Force – Целева група за Интернет инженеринг) през август 2008 г.

(2) (Изм. – ДВ, бр. 80 от 2024 г.) При вписването, заличаването или извличането, както и при предоставяне и изпращане на данни от регистър от длъжностни лица, лицата, които извършват вписването, заличаването или извличането, както и предоставянето и изпращането, се идентифицират по реда на ЗЕИ. Идентификация не се изисква за извличане на данни от публични регистри.

Изисквания към данните

Чл. 11. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Освен в случай на обоснована технологична необходимост, съгласувана с министъра на електронното управление, администрациите нямат право да пазят пълни или частични копия на данни, на които не са първични администратори.

(2) Ограничението по ал. 1 не се отнася за данни, събирани с цел предоставяне на административни услуги, както и за данни, съхранени като част от електронен документ, създаден във връзка с административно обслужване.

(3) Администрациите поддържат система за кохерентен кеш на данните за своите регистри, който:

1. съдържа най-често или най-скоро използваните данни, и

2. позволява достъп от повече от един сървър едновременно.

(4) Ако в закон е предвидено правото на лица да заявяват корекция на данни, отнасящи се за тях, съответният първичен администратор предоставя тази функционалност като електронна административна услуга.

(5) (Изм. – ДВ, бр. 80 от 2024 г.) Всеки запис в регистър има уникален идентификатор, генериран по един от следните начини:

1. съгласно стандарт RFC 4122;

2. съгласно методиката по приложение № 3;

3. друг начин, определен в нормативен акт.

(6) В информационните системи на регистрите не може да се въвежда свободен текст за данни, които представляват номенклатура или информационен обект, вписан в регистъра на информационните обекти.

Вписване и заличаване. Журнални записи

Чл. 12. (1) Всяка операция по вписване и заличаване на обстоятелство в регистър се извършва само чрез създаване на отделен нов журналин запис, отразяващ актуалното състояние.

(2) Записи, които отразяват предходни състояния, които вече не са актуални, се съхраняват с подходящ статус и информация за периода на актуалност или правно действие.

(3) Записите не подлежат на изтриване или на промяна.

(4) За всяка операция по вписване, заличаване или извличане на обстоятелства се съхранява информация за момента на извършване и за лицето, съответно информационната система, извършила операцията, освен ако данните не са публични съгласно закон.

(5) За всяка операция по ал. 4 се съхранява време, удостоверяено чрез електронен времеви печат по глава III, раздел 6 от Регламент № (ЕС) 910/2014.

(6) Интегритетът на данните по ал. 1 – 2 и 4 се защитава чрез криптографски методи.

(7) (Изм. – ДВ, бр. 80 от 2024 г.) Данните по ал. 1, 2 и 4 са достъпни за лицата, за които се отнасят, включително по електронен път, когато са се идентифицирали със средствата за електронна идентификация с ниво на осигуреност "високо", определени в Закона за електронното управление, доколкото от закон не следва друго. Достъпът се осъществява чрез потребителски и програмни интерфейси.

(8) Централният компонент по чл. 7, ал. 8 съхранява журналин запис за всяко действие, извършено чрез него.

(9) С цел предотвратяване на неоснователен достъп регистрите използват методи, с които гарантират, че е технологично неизпълнимо от тях да се извлекат данни, без това да остави журналин запис.

Обединяване на регистри

Чл. 13. Два или повече регистри могат да се водят от една или повече администрации чрез единна информационна система при спазване на нормативната уредба за съответните регистри.

Версии и управление на промените

Чл. 14. (1) Всеки програмен интерфейс по чл. 7, ал. 3 трябва да съдържа метаданни, посочващи версията му.

(2) Структурираното описание на всеки вид данни трябва да съдържа метаданни, посочващи версията му.

(3) При промяна на интерфейсите и структурите по ал. 1 и 2 съответната версия се заменя със следващата по-нова версия.

(4) В случаите по ал. 3 всички клиенти, използващи версия, различна от последната, получават информация за наличие на нова версия като част от отговора на всяка заявка.

(5) Информацията по ал. 4 се предоставя и в машинно четим формат, както и чрез портала за разработчици по чл. 61.

(6) Регистрите и базите данни поддържат активни всички версии на интерфейсите и данните си минимум 24 месеца след тяхната промяна, освен ако в закон не е предвиден друг срок.

Отворени данни

Чл. 15. (1) Регистрите и базите данни поддържат публични, свободни и безплатни интерфейси за свързани отворени данни по реда на Закона за достъп до обществена информация.

(2) Данните по ал. 1 са с максимална степен на детайлност и съдържат уникалния идентификатор на всеки запис при спазване на изискванията на относимото законодателство за защита на личните данни.

(3) При публикуването на отворени данни личните данни и друга защитена информация в публичните регистри се анонимизират, а частта от информацията, която не може да се използва повторно, съгласно чл. 41б, ал. 1 от Закона за достъп до обществена информация, не се публикува.

(4) Анонимизирането по ал. 3 се извършва чрез заменяне на съответните данни с резултата от прилагането на едноточна функция върху тях, без да се дава възможност за достигане до първоначалните данни чрез множество експериментални приложения на едноточната функция.

(5) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Интерфейсите по ал. 1 включват метаданни, определени от министъра на електронното управление.

(6) Административните органи следват препоръките на World Wide Web Consortium:

1. Добри практики за данни в уеб (Data on the Web Best Practices), 2016;

2. Добри практики за публикуване на свързани данни (Best Practices for Publishing Linked Data), 2014.

Раздел IIa

(Нов – ДВ, бр. 80 от 2024 г.)

Ред за заявяване и използване на регистър чрез Информационната система за централизирано изграждане и поддържане на регистри

Ред за заявяване на изграждането на регистър

Чл. 15а. (Нов – ДВ, бр. 80 от 2024 г.) (1) За изграждане на регистър в Информационната система за централизирано изграждане и поддържане на регистри се подава заявление по образец, одобрен от министъра на електронното управление.

(2) В случай на констатирани недостатъци в заявлението същото се връща на заявителя с указания за отстраняването им.

(3) Когато не са констатирани недостатъци и са налице основанията за изграждане на регистър в системата по ал. 1, министърът на електронното управление или упълномощено от него длъжностно лице издава заповед за изграждане на заявения регистър.

(4) В случай че към момента на разглеждане на заявлението се констатира недостатъчност на наличните технологични ресурси, в заповедта за изграждане на регистър се определя отлагателен срок, за което заявителят се уведомява.

(5) Заповедта по ал. 3 съдържа параметрите на регистъра, който ще се изгражда, и срока за изграждането му.

Използване на регистър

Чл. 15б. (Нов – ДВ, бр. 80 от 2024 г.) (1) След изграждане на регистъра по чл. 15а на заявителя или на оправомощени от него лица се предоставят необходимите права за достъп до Информационната система за централизирано изграждане и поддържане на регистри, позволяващи вписване, заличаване и промяна на данни в регистър, както и всички други операции, предвидени в нормативен акт.

(2) Миграцията на данните към изградения регистър се извършва от заявителя със съдействието на Министерството на електронното управление.

(3) Министърът на електронното управление издава технически указания за начина на миграция, вписване, заличаване, извличане, предоставяне и изпращане на данни за регистри в Информационната система за централизирано изграждане и поддържане на регистри, както и осигурява необходимите консултации.

Раздел III

Оперативна съвместимост

Общи положения

Чл. 16. (1) Информационните системи на администрациите осъществяват комуникация и други функции съгласно стандарти, описани в Регистъра на стандартите, или други стандарти и препоръки на някоя от следните организации:

1. Българския институт по стандартизация (БИС);
2. Международната организация по стандартизация (ISO);
3. Международната електротехническа комисия (IEC);
4. World Wide Web Consortium (W3C);
5. Института на инженерите по електроника и електротехника (IEEE);
6. Целевата група за интернет инженеринг (IETF);
7. Организацията за развитие на стандартите за структурирана информация (OASIS);
8. Европейския институт за стандартизация в областта на телекомуникациите (ETSI);
9. Международния съюз по телекомуникации (ITU);
10. Фондация OpenID (OIDF);
11. Групата за управление на обекти (OMG);
12. Европейския комитет по стандартизация (CEN);
13. Европейския комитет по електротехническа стандартизация (CENELEC);
14. Европейската комисия;
15. Организацията на обединените нации/Центъра за улесняване на търговията и електронния бизнес (UN/CEFACT);
16. други.

(2) За комуникация информационните системи използват формализираните описания на данни по чл. 3, ал. 2 при спазване на изискванията за управление на версии на чл. 14.

(3) За комуникация с информационни системи на други държави – членки на Европейския съюз, или на Европейската комисия се използват спецификации и протоколи, определени от Европейската комисия.

Унифициране на данни

Чл. 17. (1) Администрациите създават, обработват и предоставят данни в съответствие с формализираните описания, вписани в регистъра на информационните обекти.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление може да издава задължителни разпореждания към административните органи за промяна на информационните обекти по ал. 1.

(3) Формализираните описания на данните, които подлежат на задължително унифициране, са:

1. имена;
2. адрес;
3. единен граждански номер;
4. личен номер на чужденец;
5. ЛН – личен номер (за гражданите на Европейския съюз и техните семейства);
6. единен идентификационен код, определен от Агенцията по вписванията;
7. единен идентификационен код (код по БУЛСТАТ);
8. служебен номер по чл. 84, ал. 3 от Данъчно-осигурителния процесуален кодекс;
9. наименование на юридическо лице;
10. телефонни номера;
11. (изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) други, определени от министъра на електронното управление.

(4) Административните органи се стремят да използват формализирани описания, дефинирани от програмата ISA (ISA core vocabularies), schema.org и други стандартизирани описания.

(5) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление публикува структурите на унифицираните данни на портала за разработчици по чл. 61.

Оперативна съвместимост при обмен на документи

Чл. 18. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Обменът на електронни документи, съдържащи електронни изявления между администрациите, се извършва по технически протокол, определен от министъра на електронното управление.

(2) Протоколът по ал. 1 позволява:

1. обмен на документи между различни системи за документооборота в различни администрации;

2. проследяване на движението на документа и етапа на процедурата по разглеждането или съставянето му.

(3) Протоколът трябва да гарантира доставянето на електронните документи. В случай на спиране на работа на някой от участниците документът се изпраща не по-късно от един час от възстановяването на работата на съответния участник.

(4) Административните органи могат да използват само системи за електронен документооборот, които изпълняват протокола по ал. 1.

Глава трета

ЕЛЕКТРОННИ АДМИНИСТРАТИВНИ УСЛУГИ

Раздел I

Предоставяне на електронни административни услуги

Общи положения

Чл. 19. (1) Електронните административни услуги на администрациите се предоставят изцяло автоматизирано освен в случаите, когато е необходима експертна преценка или действие от страна на длъжностно лице.

(2) Доставчикът на електронни административни услуги предоставя информацията по чл. 13 ЗЕУ за електронните административни услуги по разбираем и достъпен начин.

(3) (Изм. – ДВ, бр. 80 от 2024 г.) Доставчикът предоставя подробна информация относно всяка предлагана от него електронна административна услуга свободно и безплатно, включително чрез официалната интернет страница на доставчика и чрез Портала на електронното управление.

(4) Електронните административни услуги се предоставят по достъпен начин, включително за лица с увреждания.

(5) При изграждане или надграждане на информационни системи за предоставяне на електронни административни услуги те задължително трябва да са на ниво 4, в случай че изискват плащане, и на ниво 3 – в останалите случаи, освен в случаите по чл. 8, ал. 3 ЗЕУ или ако в закон не е предвидено друго. Нивата на предоставяне на административните услуги се определят с § 1 от Наредбата за Административния регистър (ДВ, бр. 8 от 2016 г.).

(6) Процесите по предоставяне на електронни административни услуги следват Методологията за усъвършенстване на работните процеси за предоставяне на административни услуги, утвърдена с Решение № 578 на Министерския съвет от 2013 г.

(7) Електронните административни услуги се предоставят в съответствие с принципите на комплексното административно обслужване по смисъла на Административнопроцесуалния кодекс.

(8) Административните органи осигуряват възможност на гражданите и организациите да извършват по електронен път други правнозначими действия (разплащания, предоставяне на данни) по реда за предоставяне на електронни административни услуги.

(9) При изграждането на електронни административни услуги ръководителите на администрациите се стремят да следват следните принципи и препоръки:

1. да идентифицират нуждата от въвеждане на електронна административна услуга и анализ на потребителските потребности;
2. да използват гъвкави методологии при дефинирането и изграждането на електронни административни услуги;
3. да извършват оценка на информационната сигурност и защитата на личното пространство с оглед въвеждането на електронната административна услуга;
4. да подготвят план за действие в случай на технологична невъзможност за предоставяне на административната услуга по електронен път;
5. да насърчават гражданите да използват електронната административна услуга;
6. да събират данни за използването и потребителската удовлетвореност на електронната административна услуга.

Приемане на заявления за електронни административни услуги

Чл. 20. (1) Когато закон изисква идентификация за конкретната услуга, проверка на самоличността на заявителя при подаване на заявление по електронен път се извършва незабавно от доставчика на административни услуги по реда на ЗЕИ, както и по други начини, установени със закон.

(2) Заявление за електронна административна услуга може да се подава през публично достъпен потребителски интерфейс, през програмен интерфейс или по друг начин при наличие на съответна технологична възможност. Когато съществува внедрен програмен интерфейс за предоставяне на електронни административни услуги, административните органи са длъжни да осигурят чрез него заявяване и получаване на съответните електронни административни услуги.

(3) При липса на информационна система за приемане на заявление за определена административна услуга се допуска електронно заявяване чрез попълване на електронен документ с неструктурирано съдържание във формат по чл. 36 и изпращането му на електронната поща на доставчика на административни услуги.

(4) (Изм. – ДВ, бр. 80 от 2024 г.) Всеки административен орган оповестява чрез официалната си интернет страница и чрез Портала на електронното управление електронните адреси, на които могат да му бъдат изпращани електронни документи.

(5) (Доп. – ДВ, бр. 80 от 2024 г.) Заявлението се счита за получено от доставчика в момента на постъпване в информационната му система. Времето на получаване се отчита по реда на чл. 46.

(6) Интегритетът на заявлението и валидността на електронния подпис се установяват автоматично или по изключение – ръчно, по реда на чл. 27 от Наредбата за удостоверенията за електронен подпис в администрациите.

(7) На заявителя се дава възможност да разглежда подадените от него заявления.

(8) Заявление може да се подаде и чрез пълномощник или посредник, което се указва при заявяване на услугата. Подаващият заявлението прилага съответния документ за упълномощаване или посредничество.

(9) Когато заявлението се подава от пълномощник чрез електронно овластяване по ЗЕИ, пълномощно не се прилага.

(10) Документите, подадени по електронен път, се приемат от лица, овластени от съответните доставчици на електронни административни услуги.

Установяване на интегритет и авторство

Чл. 21. (1) В случаите, когато закон изисква заявлението за електронна административна услуга да е подписано, заявлението и приложените към него документи могат да се подписват и с усъвършенстван електронен подпис, след като физическото лице се е идентифицирало по реда на Закона за електронната идентификация.

(2) За усъвършенстван електронен подпис се счита и електронен подпис, положен чрез криптографските ключове, използвани за електронна идентификация.

(3) Когато в нормативен акт за предоставянето на административни услуги е предвидено установяване на авторството на изявления, но не чрез саморъчен подпис, за нуждите на предоставянето на електронни административни услуги авторството се установява чрез обозначеното в електронното изявление име, съответно наименование, на заявителя.

(4) Когато нормативен акт не изисква установяване на авторство на изявления за нуждите на предоставяне на електронни административни услуги, проверка за авторство не се извършва.

(5) (Изм. – ДВ, бр. 80 от 2024 г.) Интегритетът на предаваните електронни изявления през интернет чрез уеббазирани потребителски интерфейси се осигурява чрез използване на протокол HTTPS, като за установяване на криптирана връзка с потребителя на услугата се използва протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2, дефиниран в Препоръка RFC 5246, приета от IETF (The Internet Engineering Task Force – Целева група за Интернет инженеринг) през август 2008 г., или дефиниран с по-висока версия.

(6) (Доп. – ДВ, бр. 80 от 2024 г.) Интегритетът на предаваните електронни изявления през интернет чрез програмни интерфейси се осигурява чрез използване на протокол HTTPS, като за установяване на криптирана връзка с потребителя на услугата се използва протокол TLS (Transport Layer Security – Сигурност на транспортния слой), версия 1.2, дефиниран в Препоръка RFC 5246, приета от IETF (The Internet Engineering Task Force – Целева група за Интернет инженеринг) през август 2008 г., или дефиниран с по-висока версия.

(7) Интегритетът на предаваните към доставчиците на електронни административни услуги електронни изявления чрез външни носители се осигурява от получателя на електронната административна услуга.

Електронен адрес за връчване

Чл. 22. (1) Електронен адрес за връчване на резултат от електронна административна услуга е всеки адрес, на който автоматизирано може да се изпрати съобщение съгласно общоприет стандарт.

(2) Електронен адрес може да е:

1. адрес на електронна поща;

2. адрес в рамките на система за сигурно електронно връчване/система за електронна препоръчана поща;

3. адрес на програмен интерфейс, по протокол, определен от доставчика на услугата.

Портал на електронното управление

(Загл. изм. – ДВ, бр. 80 от 2024 г.)

Чл. 23. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., бр. 80 от 2024 г.) Министърът на електронното управление изгражда и поддържа Портал на електронното управление.

(2) (Изм. – ДВ, бр. 80 от 2024 г.) Порталът на електронното управление предоставя информация за всички електронни административни услуги на всички административни органи, лица, осъществяващи публични функции, и организации, предоставящи обществени услуги, както и връзка към електронна форма за тяхното заявяване.

(3) (Изм. – ДВ, бр. 80 от 2024 г.) Порталът на електронното управление използва Административния регистър по чл. 61 от Закона за администрацията за източник на актуални и достоверни данни за предоставяните административни услуги, включително електронните образци на изискуемите документи, правните основания, сроковете, тарифите и изискуемите лични данни, за предоставяне на услугите.

Електронни плащания

Чл. 24. (1) (Изм. – ДВ, бр. 80 от 2024 г.) Доставчиците на електронни административни услуги са длъжни да приемат плащания на такси във връзка с предоставяните електронни административни услуги и чрез Единната входна точка за електронни плащания в централната и местната администрация, поддържана от министъра на електронното управление, чрез електронни платежни инструменти, в съответствие със Закона за платежните услуги и платежните системи.

(2) В основанието за всяко плащане се използва уникален идентификатор, свързан с извършването на съответната услуга.

(3) Търговските банки, клоновете на чуждестранните банки и системните оператори на платежни системи са длъжни да изпращат на доставчиците на електронни административни услуги уведомление за всяко наредено плащане за електронната административна услуга независимо от начина на плащането.

(4) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., бр. 80 от 2024 г.) Потвърждението може да се извършва и чрез Единна входна точка за електронни разплащания в държавната и местната администрация, поддържана от министъра на електронното управление.

(5) (Отм. – ДВ, бр. 80 от 2024 г.).

(6) Плащането се счита за извършено, когато доставчикът на електронната административна услуга получи потвърждение от информационната система на съответния електронен платежен инструмент по ал. 1.

(7) Справката за дължими данъци и други публичноправни задължения с възможност за плащане по електронен път може да бъде вписана като административна услуга в Регистъра на услугите по Наредбата за Административния регистър.

(8) (Нова – ДВ, бр. 80 от 2024 г.) Доставчиците на електронни административни услуги предоставят възможност за плащане на електронните административни услуги чрез Централен виртуален ПОС терминал, поддържан от министъра на електронното управление. При плащане чрез Централния виртуален ПОС терминал не се дължат преводни такси и комисиони.

Изисквания за осъществяване на електронни административни услуги

Чл. 25. Доставчикът на електронни административни услуги изгражда система за предоставянето на услугите, които отговарят на следните изисквания:

1. процесът по заявяване и заплащане на електронни административни услуги да е непрекъснат, изцяло автоматизиран и да започва и да приключва в една потребителска сесия, с изключение на получаването на потвърждение за плащането;
2. да не изисква от заявителя данни, които доставчикът може да събере служебно от първичния администратор на данните;

3. от заявителя да не се изисква да прикачва сканирани хартиени документи, когато съществува възможност за извличането на информацията в тях от други информационни системи по електронен път;
4. от заявител, действащ в лично качество, да не се изисква да прикачва сканирани документи или електронни документи, подписани предварително с електронен подпис, в случаите, когато закон изисква декларирането на определени обстоятелства; декларирането на обстоятелства трябва да се извърши като част от процеса по заявяване на услугата чрез визуализиране на персонализиран електронен шаблон на изискуемата декларация и подходящ навигационен елемент за изрично потвърждаване на декларацията; декларация, потвърдена от заявителя, се прикачва в структуриран вид към целия пакет документи и заявлението и се подписва заедно с тях;
5. стъпките и полетата за попълване на заявителя да не са повече от минимално необходимите за извършването на услугата.

Общински и областни електронни административни услуги

Чл. 26. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Електронните административни услуги, предоставяни от общините и областните администрации, се изграждат по унифициран референтен модел за всички общини и областни администрации, определен от министъра на електронното управление. Министърът на електронното управление уведомява Националното сдружение на общините в Република България за референтния модел за общински услуги.

(2) Информационните системи за предоставяне на общински и областни електронни административни услуги поддържат възможност за заявяване на най-често използваните услуги към всички общини, съответно областни администрации, с една споделена инсталация без нужда от допълнителна инсталация за всяка община или областна администрация.

Електронно връчване

Чл. 27. (1) Връчване на електронни документи се извършва по реда на чл. 26 ЗЕУ.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., бр. 80 от 2024 г.) Министърът на електронното управление изгражда и поддържа система за сигурно електронно връчване като модул на Портала на електронното управление, чрез която се извършва сигурно електронно връчване на документи, свързани с електронни административни услуги.

(3) Система за сигурно електронно връчване е информационна система, която предоставя услуга за електронна препоръчана поща по смисъла на чл. 3, т. 36 от Регламент № (ЕС) 910/2014.

(4) Електронните документи, които подлежат на връчване, са документи – резултат от изпълнение на електронни административни услуги, актове, фишове, електронни фишове и наказателни постановления по смисъла на Закона за административните нарушения и наказания, както и други документи или актове, при които връчване или съобщаване се изисква от закон.

(5) Системите за сигурно електронно връчване трябва да отговарят и на следните изисквания:

1. да предоставят програмен интерфейс, чрез който друга информационна система да изпрати електронен документ за връчване, след като посочи лицето, на което да бъде връчен;
2. след успешно връчване да известяват автоматизирано по електронен път информационната система, която е изпратила електронен документ за връчване;

3. (изм. – ДВ, бр. 80 от 2024 г.) да приемат за успешно връчен само документ, който е бил отворен от лице, след като то се е идентифицирало със средствата за електронна идентификация, определени в ЗЕУ;
4. точното време на всяко действие в системата да се удостоверява чрез електронен времеви печат по глава III, раздел 6 от Регламент № (ЕС) 910/2014;
5. да гарантират неразкриването на защитена информация от трети лица.
- (6) (Нова – ДВ, бр. 80 от 2024 г.) Най-малко веднъж на две години министърът на електронното управление възлага на външен изпълнител одит на Информационната система за сигурно електронно връчване.
- (7) (Нова – ДВ, бр. 80 от 2024 г.) Одитната работа в рамките на проверката на системата за сигурно електронно връчване (CCEB) се извършва по следните направления:
1. оценка на приложимите общи контроли и контроли на ниво приложения, осигуряващи надеждността на данните в CCEB;
 2. предоставяне на увереност относно съответствието на процесите в CCEB със законодателството, политиките и стандартите, приложими за одитирания обект;
 3. предоставяне на увереност, че ИТ ресурсите обезпечават постигането на целите на организацията ефикасно и ефективно, както и че приложимите общи контроли и контроли на ниво приложения не допускат, установяват и коригират случаите на нецелесъобразно или неефективно използване и управление на CCEB.
- (8) (Нова – ДВ, бр. 80 от 2024 г.) Одитът следва да се извърши чрез подходяща комбинация от следните техники: събеседване, въпросници, наблюдение, проследяване, графики на процесите, извличане и анализ на данни, потвърждение, повторно изчисление, повторна обработка и потвърждение от трети страни. Обхватът на оценката на ИТ контролите може да включи проверка дали в CCEB са въведени:
1. структура за управление на CCEB, която функционира добре;
 2. правила за периодична инвентаризация на активите от CCEB и дали са установени нужди от разширяване;
 3. процеси за споделяне на инфраструктура и общи услуги за CCEB с други организации от публичния сектор;
 4. процес за разработване, придобиване и поддържане на CCEB (включително управление на промяната) и дали персоналят за администриране е запознат с него;
 5. процеси за ИТ операциите (вътрешно изпълнение, възлагане на подизпълнител, споразумения за обслужване), които са доведени до знанието на съответните длъжностни лица;
 6. мерки за гарантиране на физическата сигурност и адекватна физическа работна среда, както и за гарантиране на интегритета на съхраняваните данни;
 7. мерки за обучение и запознаване на персонала с въпросите, свързани с конфиденциалността, ненарушимостта и наличността на информацията, както и дали са въведени изисквания за спазване на политиката и структурата за управление на CCEB;
 8. мерки за гарантиране конфиденциалността, целостта и наличността при различните начини и канали за комуникация;
 9. мерки за управление на информационната сигурност;
 10. мерки, гарантиращи спазване на законодателството;
 11. мерки за гарантиране непрекъсваемост на дейността и възстановяване след срив;
 12. подходящи и надеждни контроли на ниво приложение за CCEB; при тази оценка може да се идентифицират съществени елементи от приложенията, критичните за CCEB приложения, да се направи преглед на наличната документация, събеседване с персонала за администриране, запознаване с контролните рискове на ниво приложения и тяхното

въздействие за ССЕСВ, както и да се разработят проверки за адекватността и надеждността на контролите на ниво приложение.

Раздел II

Посредници при предоставяне на електронни административни услуги

Общи положения

Чл. 28. (1) (Отм. – ДВ, бр. 80 от 2024 г.).

(2) (Изм. – ДВ, бр. 80 от 2024 г.) Посредникът подпомага процеса на заявяване на съответната услуга.

(3) Посредникът действа с оглед максимална защита на интересите на заявителя.

Изисквания към дейността на посредниците

Чл. 29. (1) (Изм. – ДВ, бр. 80 от 2024 г.) Посредникът организира дейността си по начин, който осигурява обслужване на потребителите на административни услуги на място, лесно за намиране и достъп.

(2) Посредникът:

1. предоставя информация за електронните административни услуги на достъпен и разбираем език;
2. отговаря на запитвания от общ характер;
3. разяснява изискванията, на които трябва да отговаря заявлението за заявяване на електронните административни услуги;
4. (доп. – ДВ, бр. 80 от 2024 г.) попълва и изпраща заявленията за електронна административна услуга по електронен път;
5. дава информация за хода на работата по преписката;
6. информира получателите на електронни административни услуги за условията и особеностите на получаването им, включително за актовете – резултат от услугите, както и за процедурите за подаване на жалби и за решаване на спорове във връзка със съответните услуги;
7. (нова – ДВ, бр. 80 от 2024 г.) информира за дължимите такси за електронната административна услуга, ако такива са определени от доставчика на услугата, като същите са за сметка на получателя на услугата;
8. (нова – ДВ, бр. 80 от 2024 г.) информира получателите на електронни административни услуги относно дължимото възнаграждение за посредничество по ясен и разбираем начин.

(3) Посредникът трябва да притежава удостоверение за квалифициран електронен подпис, което да бъде използвано във връзка с дейността му на посредник при електронни административни услуги.

(4) По искане на посредника доставчикът на електронни административни услуги му предоставя образец на заявление и актуална информация в обем, необходим и достатъчен за изпълнение на дейностите по заявяване на електронната услуга.

(5) (Нова – ДВ, бр. 80 от 2024 г.) Посредникът трябва да разполага с технически средства, необходими за заявяването на електронната административна услуга.

(6) (Нова – ДВ, бр. 80 от 2024 г.) Посредникът извършва плащането към доставчика за заявената услуга в съответствие с чл. 24.

Процедура за заявяване и получаване на електронни административни услуги чрез посредник

Чл. 30. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., доп., бр. 80 от 2024 г.)

Отношенията между посредника и заявителя възникват въз основа на писмен договор. Министърът на електронното управление утвърждава образец на писмен договор.

- (2) Посредникът проверява чрез допустимите средства самоличността на получателя на електронната услуга и ако е необходимо – други данни за тези лица, необходими за ползването на услугата.
- (3) При заявено получаване чрез лицензиран пощенски оператор издаденият индивидуален административен акт се изпраща по реда на чл. 7, ал. 5 от Наредбата за административното обслужване.
- (4) (Нова – ДВ, бр. 80 от 2024 г.) Министърът на електронното управление води публичен списък на посредниците при заявяване на електронни административни услуги.
- (5) (Нова – ДВ, бр. 80 от 2024 г.) За включване и изключване от списъка по ал. 4 посредникът подава заявление до министъра на електронното управление.

Такси и възнаграждения за посредничество

- Чл. 31. (1) Дължимите такси за ползване на електронна административна услуга, ако такива са определени от доставчика на услугата, са за сметка на получателя на услугата.
- (2) Дължимите такси се заплащат по банков или електронен път или на каса при посредника – с банкова карта или в брой. При заплащане на услугата по банков път получателят представя идентификатор на извършеното плащане.
- (3) Приемането на дължими такси и други публичноправни задължения от посредника и заплащането им към доставчиците на електронни административни услуги се извършват съгласно действащото законодателство.
- (4) Посредникът при заявяване на електронни административни услуги може да осъществява дейността си срещу възнаграждение.
- (5) Посредникът информира получателя на електронната административна услуга относно дължимото възнаграждение за посредничество по ясен и разбираем начин преди възлагането на представителството.

Глава четвърта ОБМЕН НА ЕЛЕКТРОННИ ДОКУМЕНТИ В АДМИНИСТРАЦИИТЕ

Общи положения

- Чл. 32. (1) Административните органи са длъжни да използват система за електронен документооборот и да участват в електронен обмен на документи с други администрации.
- (2) Не се допуска обмен на документи на хартиен носител, освен в случаите, когато това е определено със закон.
- (3) Обменът на електронни документи се извършва между участници, регистрирани в Административния регистър.
- (4) Обменът на електронни документи се извършва чрез протокола по чл. 18, ал. 1, като протоколът се публикува на портала за разработчици по чл. 61.
- (5) При обмен на електронни документи всички участници са равнопоставени.
- (6) Електронните документи и техни резервни копия се съхраняват за срок, определен от съответния ръководител, освен ако в закон не е определен срок за съхраняване на съответния документ. След изтичане на срока се архивират според правилата по чл. 43.
- (7) Административните органи са длъжни да използват и системи за бази данни за знание с възможност за пълнотекстово търсене, където да съхраняват електронни документи, описващи всички процедури и добри практики, отнасящи се до дейността им.
- (8) Достъпът до системите по ал. 7 е свободен и безплатен за всички администрации.

Изисквания към обмена на електронни документи

Чл. 33. (1) Обменът на електронни документи се извършва чрез директна комуникация между системите за електронен документооборот на участващите администрации.

(2) Обменът се извършва чрез криптирана връзка по начин, определен с протокола по чл. 18, ал. 1.

(3) Обменът се осъществява в съответствие с Наредбата за обмена на документи в администрацията.

(4) Идентификацията на системите за електронен документооборот се извършва чрез удостоверенията на съответните администрации по реда на чл. 10, ал. 1 и 2.

(5) В обмена може да участва и централен компонент, който получава информация от участниците. Централният компонент задължително се поддържа в тестови режим, както и в режим за експериментална интеграция.

Изисквания към системите за електронен документооборот

Чл. 34. (1) Системите за електронен документооборот трябва да поддържат протокола по чл. 18, ал. 1.

(2) Достъпът до системите на длъжностните лица се извършва по реда на ЗЕИ.

(3) (Изм. – ДВ, бр. 80 от 2024 г.) Системите трябва да позволят подписване на документите с електронен подпис по реда на Закона за електронния документ и електронните удостоверителни услуги и на тази наредба.

(4) Системите трябва да предоставят програмни интерфейси за достъп до своите преписки и документи, както и за получаване на входящи номера и регистриране на преписки.

(5) Системите трябва да съхраняват информация за всяка процедура по обмен на електронни документи, включително с електронен времеви печат по глава III, раздел 6 от Регламент № (ЕС) 910/2014.

(6) Информацията по ал. 4 не подлежи на изтриване и модификация и интегритетът ѝ се защитава чрез криптографски методи.

Подаване на документи от граждани и организации

Чл. 35. (1) Системите за електронен документооборот могат да поддържат и приемане на документи от граждани и организации по електронен път.

(2) Приемането се осъществява чрез публичен интерфейс, отговарящ на изискванията за ползваемост по глава пета.

Видове и формати на електронните документи

Чл. 36. (1) Електронните документи могат да бъдат със структурирано и с неструктурирано съдържание и трябва да използват отворени формати.

(2) Електронните документи със структурирано съдържание са електронни документи, които имат предварително дефинирана структура посредством общоприет стандарт и които отговарят на изискванията на протокола по чл. 18, ал. 1.

(3) Електронните документи с неструктурирано съдържание са всички електронни документи извън тези по ал. 2.

(4) За текстови документи, електронни таблици и презентационни документи се използва ISO/IEC 26300 – OASIS Open Document Format for Office Application, освен ако няма обоснована технологична необходимост от друг формат.

Електронно подписване на документи в администрацията

Чл. 37. (1) Електронните документи се подписват с електронен подпис, издаден по реда на Наредбата за удостоверенията за електронен подпис в администрациите.

(2) Проверката на интегритета на документите и на валидността на електронния подпис става автоматично или по изключение – от определено длъжностно лице, по реда на чл. 27 от Наредбата за удостоверенията за електронен подпис в администрациите.

(3) За електронно подписване на XML базирани документи се използва форматът XAdES (XML Advanced Electronic Signature), формулиран в стандарт Final draft ETSI EN 319 132-1 V1.1.0 February 2016 – Препоръка TS 101 903 от април 2004 г. на ETSI (European Telecommunications Standards Institute – Европейски институт за стандартизация в телекомуникациите), и основан на Препоръка XML Signature Syntax and Processing (Синтаксис и обработка на XML подписи), приета от консорциума W3C (World Wide Web Consortium – Консорциум на световната мрежа) на 12 февруари 2002 г.

Глава пета

ОБЩИ ИЗИСКВАНИЯ КЪМ ИНФОРМАЦИОННИТЕ СИСТЕМИ И СОФТУЕРНИТЕ КОМПОНЕНТИ

Общи положения

Чл. 38. (1) Всички информационни системи и софтуерните компоненти в администрацията, в т.ч. регистри, интернет страници, вътрешни информационни системи, потребителски интерфейси към съществуващи системи, системи за предоставяне на електронни административни услуги и за електронен документооборот, трябва да отговарят на изискванията на тази глава.

(2) (Изм. – ДВ, бр. 80 от 2024 г.) Общите и специфичните изисквания към системите според тази наредба се включват в техническата спецификация при разработка, надграждане или внедряване на системи.

(3) (Изм. – ДВ, бр. 80 от 2024 г.) При изготвяне на спецификации за провеждане на обществени поръчки, чийто обхват включва разработка, надграждане или внедряване на софтуерни компоненти и софтуерната част на информационни системи, възложителите изготвят техническите си задания и спецификации на базата на образец съгласно приложение № 1.

(4) (Нова – ДВ, бр. 80 от 2024 г.) При изготвяне на технически спецификации за провеждане на обществени поръчки, чийто обхват включва само дейности по адаптиране на информационни системи, регистри или бази данни във връзка с въвеждане на еврото в Република България, възложителите могат да изготвят техническите си спецификации на базата на образец съгласно приложение № 2. В случаите, когато в техническите спецификации са включени и други дейности, се прилага ал. 3.

(5) (Предидшна ал. 4, доп. – ДВ, бр. 80 от 2024 г.) Образецът по ал. 3 се използва независимо дали в рамките на поръчката са включени и дейности, свързани хардуер, мрежова инфраструктура и др.

(6) (Предидшна ал. 5, изм. – ДВ, бр. 80 от 2024 г.) Образците по ал. 3 и 4 могат да се изменят и допълват съобразно дейностите и услугите в обхвата на обществената поръчка и конкретните изисквания на възложителите.

(7) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., предидшна ал. 6, изм., бр. 80 от 2024 г.) Министърът на електронното управление публикува образците по ал. 3 и 4 в електронна форма на интернет страницата на министерството.

(8) (Предидшна ал. 7, изм. – ДВ, бр. 80 от 2024 г.) При вътрешна разработка, надграждане или внедряване на информационни системи и софтуерни компоненти администрациите спазват изискванията, включени в образците по ал. 3 и 4.

Ред за извеждане на информационни системи от експлоатация

Чл. 38а. (Нов – ДВ, бр. 80 от 2024 г.) Информационни системи се извеждат от експлоатация при спазване на следния ред:

1. административният орган издава заповед за извеждане от експлоатация на информационните системи, за които не са предвидени средства за поддържането им;
2. прекратява се достъпът до данните и функционалностите на информационната система;
3. информационната система с данните в нея се архивира към момента на извеждането ѝ от експлоатация.

Ползваемост и достъпност

Чл. 39. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление утвърждава препоръки към потребителските интерфейси.

(2) (Изм. – ДВ, бр. 4 от 2020 г., в сила от 14.01.2020 г., бр. 80 от 2024 г.) Съдържанието на интернет страниците и мобилните приложения на административните органи, на доставчиците на обществени услуги и на лицата, осъществяващи публични функции, трябва да отговаря на последната обнародвана в "Официален вестник" на Европейския съюз версия на хармонизирания стандарт EN 301 549, освен в случаите по чл. 58в, ал. 2 или 3 от ЗЕУ.

(3) Потребителските интерфейси на публичните елементи от информационните системи и интернет страниците трябва да бъдат с адаптивен дизайн и структура, така че да са достъпни и удобни за обичайна употреба както от мобилни устройства, така и от настолни устройства.

(4) (Изм. – ДВ, бр. 4 от 2020 г., в сила от 14.01.2020 г.) Административните органи, доставчиците на обществени услуги и лицата, осъществяващи публични функции, разработват и публикуват декларация за достъпност по чл. 58в, ал. 4 от ЗЕУ, която задължително съдържа описание на:

1. статуса на съответствие на съдържанието на интернет страница или мобилно приложение със стандарта по ал. 2;
2. частите на съдържанието, които не са достъпни, и причините за това, както и предвидени достъпни алтернативи, когато това е целесъобразно;
3. метода, използван за изготвяне на декларацията;
4. механизма за предоставяне на обратна информация и данни за контакт – за нотификация от гражданите при наличие на съдържание, което не отговаря на изискванията за достъпност;
5. процедурата по прилагане в случай на неудовлетворителен отговор на нотификацията.

Изключения от задължението за достъпност поради прекомерна тежест

Чл. 39а. (Нов – ДВ, бр. 4 от 2020 г., в сила от 14.01.2020 г.) (1) Мерки, водещи до прекомерна тежест, са тези, които биха наложили прекомерна организационна или финансова тежест за задължения субект или биха застрашили способността му да изпълни своята цел или да публикува информация, която е необходима за неговите задължения и услуги или е свързана с тях, като същевременно се взема предвид вероятната полза или вреда, която би настъпила за гражданите, по-специално за хората с увреждания.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Ако конкретен задължен субект иска да приложи изключението от изпълнението на чл. 39, ал. 2 поради прекомерна тежест, трябва да извърши първоначална оценка на степента, до която спазването на изискванията за достъпност води до прекомерна тежест, и да я предостави за одобряване с доклад до министъра на електронното управление.

(3) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Докладът се разглежда по процедура, определена от министъра на електронното управление.

(4) В случай че извършената оценка бъде одобрена, в декларацията за достъпност за съответната интернет страница или мобилното приложение задълженият субект подробно описва елементите от изискванията за достъпност, които не е бил в състояние да изпълни, и предлага достъпни алтернативи, когато е целесъобразно. Оценката се преразглежда от

задължения субект най-малко веднъж годишно, за да бъдат взети предвид възможни организационни или технически промени.

(5) За да се оцени до каква степен спазването на изискванията за достъпност по чл. 39, ал. 2 води до прекомерна тежест, задължените субекти трябва да вземат предвид най-малко следните обстоятелства:

1. размера, ресурсите и естеството на съответния задължен субект;
2. прогнозните разходи и ползи за съответния задължен субект спрямо прогнозните ползи за хората с увреждания, като се отчитат честотата и продължителността на използване на конкретната уеб страница или мобилно приложение.

(6) Липсата на приоритет, време или знания не се считат за основания за изключение поради прекомерна тежест.

(7) Изключенията от изпълнението на изискванията за достъпност по чл. 39, ал. 2 поради прекомерна тежест трябва да бъдат ограничени до конкретно съдържание и определени части с цел намаляване на тежестта, като същите трябва да бъдат обосновани. Независимо от това задълженият субект трябва да направи това съдържание възможно най-достъпно.

Институционална идентичност

Чл. 40. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Интернет страниците на администрациите трябва отговарят на правилата за институционална идентичност, определени от министъра на електронното управление.

(2) Правилата съдържат изисквания най-малко за следните компоненти:

1. разположението на наименованието и символите на администрацията;
2. съдържанието и поредността на елементите в менютата;
3. навигационната структура на интернет страниците;
4. разполагането на банери с връзки към други интернет страници;
5. метаданните за обработване при автоматизирано търсене, както и други метаданни за използване от външни приложения.

Софтуерна архитектура

Чл. 41. (1) Всяка функционалност на сървърните компоненти на системите, която е достъпна за потребителите, трябва да е достъпна и като публичен програмен интерфейс чрез уебслужба.

(2) Всички системи трябва да комуникират помежду си единствено с публично документиран програмни интерфейси. Достъпът до програмните интерфейси се определя от ръководителя на съответната администрация.

(3) Публичните програмни интерфейси трябва да поддържат атрибут за версия. Старите версии трябва да са достъпни минимум 24 месеца след публикуването на нова версия.

(4) Когато обхватът на системата предполага използване от повече от една администрация, то системата трябва да е изградена така, че с една инсталация да могат да бъдат обслужвани съответните администрации.

(5) Инсталирането на нова версия на системите трябва да се извършва, без те да спират работа.

(6) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) В извънредни случаи, когато технологични причини налагат това, спирането на работата на системата се извършва извън работното време на администрацията, като за това се уведомяват министърът на електронното управление и всички заинтересовани страни не по-късно от два работни дни преди спирането.

Резервни копия

Чл. 42. (1) Длъжностно лице, определено от съответния ръководител, осигурява автоматизираното създаване на резервни копия на всички данни и електронни документи най-малко всеки ден. Допуска се създаване на копия само на новите и променените данни и документи.

(2) Резервните копия се съхраняват на носител, различен от този, на който са разположени данните или електронните документи.

(3) Съхраняват се най-малко последните три резервни копия.

(4) Резервните копия се криптират с публичния ключ на съответната администрация.

(5) Резервните копия се изпитват за консистентност и интегритет чрез пробно възстановяване на данни най-малко веднъж месечно.

Дългосрочно съхранение на електронни документи

Чл. 43. (1) На дългосрочно съхранение подлежат електронни документи, по-стари от две години, чийто срок на валидност е изтекъл, освен ако в закон не е предвидено друго.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление изготвя насоки за дългосрочно съхранение на електронни документи.

Отворен код, документация и авторски права

Чл. 44. (1) Системите по чл. 58а, т. 1 ЗЕУ се разработват с отворен код от началото на всеки проект за изграждане или надграждане.

(2) Изходният код и документацията на системите се предоставят публично в обем на авторските права под един от следните лицензи:

1. EUPL (European Union Public License);
2. GPL (General Public License) 3.0;
3. LGPL (Lesser General Public License);
4. AGPL (Affero General Public License);
5. Apache License 2.0;
6. New BSD license;
7. MIT License;
8. Mozilla Public License 2.0.

(3) Авторските права върху разработените системи и софтуерни компоненти трябва да бъдат уредени в проекта на договор по чл. 31, ал. 1, т. 5 от Закона за обществените поръчки и трябва да възникват в пълен обем за възложителя като произведения, създадени по поръчка по смисъла на чл. 42 от Закона за авторското право и сродните му права.

Информационна сигурност

Чл. 45. (Изм. – ДВ, бр. 80 от 2024 г.) (1) Всички доставчици на електронни административни услуги са длъжни да спазват изискванията на Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност.

(2) Лицата, водещи регистри по смисъла на чл. 4а, ал. 2 от ЗЕУ, веднъж годишно провеждат тест за външно проникване в сигурността, извършен от независима организация.

Отчитане на астрономическо време

Чл. 46. (1) Информационните системи отчитат астрономическото време по стандарт UTC (Coordinated Universal Time), базиран на Препоръка 460-4 "Standard Frequency and Time Signal Emissions – Стандартна честота и излъчване на времеви сигнал" от 1986 г. на Международния съюз по телекомуникации (ITU – International Telecommunications Union).

(2) Времето за настъпването на факти с правно или техническо значение се отчита с точност до година, дата, час, минута и секунда, изписани в съответствие със стандарта БДС ISO 8601:2006. При технологична необходимост се допуска и отчитане до милисекунда.

- (3) Времето се отчита по националната часова зона (UTC+2).
- (4) При комуникация с информационни системи на други държави – членки на Европейския съюз, или на Европейската комисия времето се отчита по съответния стандарт, определен от Европейската комисия.
- (5) За синхронизация на часовниците на мрежовите сървъри, използвани от доставчиците на електронни административни услуги, трябва да се използва протоколът NTP V4 (Network Time Protocol, версия 4.0 и сл.), основан на Препоръка RFC 1305, приета от IETF (The Internet Engineering Task Force – Целева група за интернет инженеринг) през март 1992 г., като се осигурява хронометрична детерминация с времевата скала на UTC, или аналогичен.
- (6) Изискванията за отчитане на астрономическо време се отнасят и до информационните системи на лицата, осъществяващи публични функции, и до организациите, предоставящи обществени услуги.
- (7) Астрономическото време в информационните системи се отчита от сървъра.

Наименования на домейни

Чл. 47. (1) Наименованията на домейните и поддомейните, използвани от административните органи, се определят от съответния ръководител.

(2) Интернет страниците на административните органи трябва да са достъпни чрез домейн, формиран както чрез префикса "www" ("World Wide Web"), определен като стандарт от консорциума W3C ("World Wide Web Consortium"), така и без него.

(3) Официалните домейни, използвани от административните органи, трябва да са в националните домейни от първо ниво (ccTLD) – ".bg" на латиница и ".бг" на кирилица, или да са поддомейни на "government.bg".

(4) Интернет страниците, които са достъпни чрез поддомейн на домейн "government.bg", трябва да са достъпни и чрез същия поддомейн на домейни "gov.bg" и "правителство.бг". Поддомейните на "правителство.бг" трябва да са на кирилица.

(5) Официалните страници на централните администрации могат да са достъпни чрез отделни домейни или като поддомейни на "government.bg".

(6) При формиране на наименованията на домейните и поддомейните, както и на адресите на електронна поща, използвани от областните администрации, се прилагат съответно правилата по ал. 2 – 4, както и следните правила:

1. официалните домейни, използвани от областните администрации, трябва да са поддомейни на "government.bg";

2. официалните домейни, използвани от областните администрации, трябва да се формират от транслитерацията на наименованието на съответния областен град; наименованията на домейните на Софийска област са "www.sofia-oblast.government.bg" и "www.sofia-region.government.bg".

(7) При формиране на наименованията на домейните и поддомейните, както и на адресите на електронна поща, използвани от общинските администрации, се прилагат съответно правилата по ал. 2 – 4, както и следните правила:

1. официалните домейни, използвани от общинските администрации, трябва да се формират от транслитерацията на наименованието на съответната община, както и с изписването им на кирилица;

2. ако домейнът, формиран по правилата на т. 1, е зает от друга организация, официалният домейн, използван от съответната общинска администрация, се формира, като към наименованието на съответната община се добавя думата "град" или думата "община", транслитерирани по реда на Закона за транслитерацията, както и с изписването им на кирилица.

(8) Интернет страниците на общинските съвети трябва да са достъпни от интернет страниците на съответните общински администрации, ако се поддържат отделно. В този случай наименованията на домейните се формират с използване на префикс метод по следния начин: "www.savet.sofia.bg", "savet.sofia.bg" и "съвет.софия.бг", съответно.

(9) (Нова – ДВ, бр. 80 от 2024 г.) Държавният хибриден частен облак (ДХЧО) предоставя услугите си в домейн egov.bg.

(10) (Нова – ДВ, бр. 80 от 2024 г.) Хоризонталните системи на електронното управление се публикуват на поддомейни на egov.bg със следната конвенция: [име на хоризонтална система].egov.bg.

(11) (Нова – ДВ, бр. 80 от 2024 г.) Администрациите, които използват ресурси от ДХЧО, могат да публикуват в egov.bg системи за общ достъп като поддомейни със следната конвенция: [име на система].egov.bg.

Глава шеста

РЕГИСТРИ И СИСТЕМИ НА МИНИСТЕРСТВОТО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

(Загл. изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.)

Раздел I

Информационна система за предварителен, текущ и последващ контрол по целесъобразност

Общи положения

Чл. 48. (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) (1) (Предишен текст на чл. 48 – ДВ, бр. 80 от 2024 г.) Информационна система за предварителен, текущ и последващ контрол по целесъобразност в областта на електронното управление и използването на информационните и комуникационните технологии в дейността на административните органи и техните администрации е публична и се изгражда и поддържа от министъра на електронното управление.

(2) (Нова – ДВ, бр. 80 от 2024 г.) Министърът на електронното управление утвърждава правила за предварително съгласуване на разходите на административните органи в областта на електронното управление и за използваните от тях информационни и комуникационни технологии в рамките на бюджетния процес.

Подлежащи на вписване обстоятелства

Чл. 49. (Изм. – ДВ, бр. 80 от 2024 г.) За нуждите на информационната система по чл. 48 на вписване подлежи предоставяната от административните органи информация за:

1. средносрочните бюджетни прогнози;
2. проектобюджетите за следващата година;
3. утвърдените годишни бюджети;
4. промени по утвърдените бюджети;
5. текущите отчети;
6. годишния отчет.

Вписване и съгласуване

Чл. 50. (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., бр. 80 от 2024 г.) (1) Първостепенните разпоредители с бюджет определят длъжностни лица, които вписват информацията по чл. 49 в системата по чл. 48.

(2) Лицата по ал. 1 – за централната администрация, вписват информацията по чл. 49 в срокове, както следва:

1. по т. 1 – средносрочните бюджетни прогнози – в 10-дневен срок от датата на утвърждаване на указанията на министъра на финансите за подготовката и предоставянето на бюджетните прогнози на първостепенните разпоредители с бюджет;
 2. по т. 2 – проектобюджетите за следващата година и актуализираните им бюджетни прогнози – в 10-дневен срок от датата на указанията на министъра на финансите за подготовката и представянето на проектобюджетите на първостепенните разпоредители с бюджет и актуализираните им бюджетни прогнози;
 3. по т. 3 – утвърдените бюджети – в едномесечен срок от обнародването на постановлението за изпълнението на Закона за държавния бюджет на Република България за съответната година;
 4. по т. 4 – извършване на промени по утвърдените бюджети – в 15-дневен срок до извършването на промените по бюджетите по реда на Закона за публичните финанси;
 5. по т. 5 – текущите отчети – в 7-дневен срок от представянето на тримесечните отчети за касовото изпълнение чрез Информационната система за Управление на държавното съкровище на Министерството на финансите;
 6. по т. 6 – годишен отчет – в 15-дневен срок от получаването на окончателния одитен доклад и одитното становище на Сметната палата.
- (3) Лицата по ал. 1 – за общинската администрация, вписват информацията по чл. 49 в срокове, както следва:
1. по т. 1 – средносрочните бюджетни прогнози – преди внасянето на прогнозите в общинските съвети за приемане;
 2. по т. 2 – проектобюджетите за следващата година и актуализираните им бюджетни прогнози – преди внасянето на проектобюджетите на първостепенните разпоредители с бюджет и актуализираните им бюджетни прогнози в общинските съвети за приемане;
 3. по т. 3 – утвърдените бюджети – в едномесечен срок от приемането на общинския бюджет;
 4. по т. 4 – извършване на промени по утвърдените бюджети – преди внасянето им в общинските съвети за приемане;
 5. по т. 5 – текущите отчети – в 7-дневен срок от представянето на отчета за всяко шестмесечие за касово изпълнение чрез Информационната система за общините на Министерството на финансите;
 6. по т. 6 – годишен отчет – в 15-дневен срок от приемането им от общинските съвети.
- (4) Министърът на електронното управление съгласува вписаните данни по ал. 2 и 3 в 14-дневен срок от вписването им.
- (5) В случай на връщане към административния орган на коментари относно подадената от него информация по чл. 49 съответният първостепенен разпоредител с бюджет отразява бележките на министъра на електронното управление и вписва променените данни в системата по чл. 48. При частично или пълно неприемане на коментарите съответната администрация изготвя мотивирано становище и го изпраща до министъра на електронното управление чрез системата по чл. 48.
- (6) В случай на мотивиран отказ за съгласуване по целесъобразност съответният първостепенен разпоредител с бюджет може да обжалва решението за отказ или да впише наново преработена съгласно забележките информация.

Раздел II

Регистър на проекти и дейности

Обхват

Чл. 51. Регистърът на проектите и дейностите е публична електронна база данни и съдържа данни за всички проекти и дейности в областта на електронното управление и информационните и комуникационните технологии в администрациите.

Вписване

Чл. 52. (Изм. – ДВ, бр. 80 от 2024 г.) (1) В регистъра по чл. 51 се вписват данни и информация съгласно чл. 7д, ал. 1 и 2 от ЗЕУ, включително необходимите за извършване на проверка на проектни предложения и дейности, включени в правилата по чл. 53, ал. 2, на следните етапи като минимум:

1. проектни предложения и дейности:

а) общите и специфичните цели;

б) съответствие със стратегически и програмни документи в областта на електронното управление;

в) пълно описание на дейностите в областта на електронното управление, информационните и комуникационните технологии в администрациите;

г) очакваните резултати и измеримите индикатори за резултат, включително по отношение на гражданите и бизнеса;

д) необходими изменения на нормативната рамка за осигуряване на съответствие със законодателството за електронното управление;

е) план-график и индикативен бюджет;

2. техническите спецификации за обществени поръчки по чл. 58а от ЗЕУ;

3. оценка на качеството на изпълнение на проекта, постигнатите резултати и финансов ефект.

(2) Ръководителите на администрациите определят длъжностни лица, които извършват вписването в регистъра по чл. 51.

(3) Лицата по ал. 2 вписват данните по ал. 1, т. 1 и 2:

1. преди публикуването на обществената поръчка в Регистъра на обществените поръчки, или

2. преди изпращането на заявка по действащо рамково споразумение.

(4) В случаите, когато проектното предложение или дейността се финансира със средства от Европейския съюз и от други международни програми и договори, лицата по ал. 2 вписват данните по ал. 1, т. 1 преди изпращането на проектното предложение (дейността) за оценка към финансиращата организация.

(5) Лицата по ал. 2 вписват данните по ал. 1, т. 3 в срок 30 дни от приемане от възложителя на резултатите от проекта/дейността.

Утвърждаване на проектни предложения и дейности

(Загл. доп. – ДВ, бр. 80 от 2024 г.)

Чл. 53. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., бр. 80 от 2024 г.) Министърът на електронното управление утвърждава проектните предложения или дейности, както и удостоверява съответствие с изискванията на чл. 58а от ЗЕУ на технически спецификации, вписани в регистъра по чл. 51, в двуседмичен срок от вписването им.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., изм. и доп., бр. 80 от 2024 г.) Министърът на електронното управление утвърждава правила за извършване на проверки на проектни предложения и дейности, както и на технически спецификации за обществени поръчки по чл. 58а от ЗЕУ.

(3) (Отм. – ДВ, бр. 80 от 2024 г.).

(4) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., бр. 80 от 2024 г.) Ако проектното предложение, дейността или техническата спецификация съдържат несъответствия с нормативните изисквания, министърът на електронното управление или определено от него длъжностно лице дава предписания за отстраняването им от вписалата ги администрация в едномесечен срок.

(5) (Доп. – ДВ, бр. 80 от 2024 г.) Отказът да се утвърди проектно предложение или дейност или да се удостовери съответствие с изискванията на чл. 58а от ЗЕУ на техническа спецификация се мотивира и се вписва в регистъра по ал. 1 заедно с мотивите.

(6) (Изм. – ДВ, бр. 80 от 2024 г.) Отказите по ал. 5 подлежат на обжалване в 14-дневен срок от съобщаването им по реда на Административнопроцесуалния кодекс.

(7) При липса на отказ проектното предложение се счита за утвърдено.

(8) (Изм. – ДВ, бр. 80 от 2024 г.) Регистърът съдържа данни за:

1. всички утвърдени проекти и дейности, както и проектни предложения и дейности с постановен отказ за утвърждаване;
2. всички технически спецификации за обществени поръчки по чл. 58а от ЗЕУ.

Достъп до регистъра

Чл. 54. (1) Достъпът до регистъра е свободен и безплатен.

(2) Регистърът предоставя публична справочна функционалност и функционалност за пълнотекстово търсене.

(3) Регистърът позволява абониране за известия по определени критерии. Известията се изпращат чрез уебслужби, по електронна поща или RSS (Rich Site Summary) или еквивалентен стандарт.

Раздел III

Регистър на информационните ресурси

Обхват

Чл. 55. (1) Регистърът на информационните ресурси е електронна база данни и съдържа данни за всички информационни ресурси в държавната администрация, в т.ч. единната електронна съобщителна мрежа на държавната администрация, с изключение на тези, чието предназначение е за работа и съхранение на класифицирана информация.

(2) Информационни ресурси са:

1. хардуер, в т.ч. сървъри, настолни и мобилни компютри и устройства;
2. мрежово оборудване;
3. софтуер;
4. софтуерни лицензи.

(3) За всеки хардуерен и мрежови информационен ресурс се поддържат най-малко следните метаданни:

1. вид;
2. марка и модел;
3. продуктов номер;
4. сериен номер;
5. производител;
6. доставчик;
7. година на производство;
8. година на закупуване;
9. срок на гаранционна поддръжка;
10. история и условията на гаранционната и извънгаранционната поддръжка;
11. цена на придобиване;
12. разходи за извънгаранционна поддръжка.

(4) За всеки софтуер се поддържат най-малко следните метаданни:

1. фирма-разработчик или отдел (вътрешен изпълнител);
2. изходен код или връзка към хранилището по чл. 58, ал. 2, ако са налични;
3. година на изграждане;

4. срок на гаранционна поддръжка;
5. история и условия на гаранционната и извънгаранционната поддръжка;
6. версия;
7. договори за разработка и надграждане;
8. други свързани със софтуера информационни ресурси;
9. цена;
10. разходи за извънгаранционна поддръжка.

(5) За всеки вид лицензиран софтуерен продукт се поддържат най-малко следните данни:

1. разработчик;
2. доставчик;
3. срок;
4. използвана и максимална възможна версия;
5. условия за ползване;
6. брой закупени лицензи;
7. тип на лицензирането (на процесор, на ядро, на работна станция, на инсталация и др.);
8. единична цена.

(6) Годишните планове за обновяване на информационните ресурси за всеки от видовете по ал. 3 – 5, като за годишния план за всеки ресурс или група ресурси се вписва:

1. планираният месец на обновяване;
2. причината за обновяване;
3. планираният бюджет.

(7) Регистърът се съхранява безсрочно.

Вписване и заличаване

Чл. 56. (1) Административните органи са длъжни да вписват в регистъра по чл. 55, ал. 1 данните за информационните ресурси в едномесечен срок от въвеждането, съответно от извеждането им от експлоатация.

(2) Вписването и заличаването се извършват чрез потребителски или програмен интерфейс на регистъра, както и чрез регистъра по чл. 51 след приключването на проект или дейност, резултатът от които подлежи на вписване в регистъра по чл. 55.

(3) Потребителският и програмният интерфейс на регистъра позволяват обмен на вписани и заличени данни с външни информационни системи.

(4) Ръководителите на администрациите определят длъжностни лица, които извършват вписването и заличаването или отговарят за автоматизираното вписване и заличаване.

(5) Автоматизираното вписване и заличаване се извършват чрез програмния интерфейс по ал. 2.

(6) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление възлага проверки и одити за установяване на актуалността на вписаната в регистъра информация.

Достъп до регистъра

Чл. 57. (1) Достъп до регистъра имат:

1. (изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) министърът на електронното управление и определени от него лица – до пълното съдържание на регистъра;
2. ръководителите на администрациите и определени от тях лица – до данните за съответната администрация;
3. всяко лице – до справочни данни и данни за всички ресурси, с изключение на данни за модели, продуктови и серийни номера.

(2) Регистърът предоставя агрегирани справки по всички комбинации от вписани обстоятелства, в т.ч. администрации, за които се отнасят.

Раздел IV

Хранилище за изходен код

Общи положения

Чл. 58. (1) Хранилището за изходен код е информационна система за съхранение и достъп до изходен код, включваща система за контрол на версиите.

(2) Хранилището позволява неограничен брой проектни хранилища, като всяко проектно хранилище се отнася за един проект.

(3) Всяко проектно хранилище се отнася към определена администрация.

(4) В хранилището се съхранява кодът на всички проекти или части от проекти, разработени за администрацията по поръчка, отговаряща на условията на чл. 58а, т. 1 ЗЕУ.

Управление и достъп до хранилището

Чл. 59. (1) (Нова – ДВ, бр. 80 от 2024 г.) Министърът на електронното управление изгражда и поддържа хранилището за изходен код на интернет адрес: git.egov.bg.

(2) (Предишна ал. 1 – ДВ, бр. 80 от 2024 г.) Достъпът до изходния код в хранилището е свободен и безплатен.

(3) (Предишна ал. 2 – ДВ, бр. 80 от 2024 г.) Използването на изходен код се урежда от избрания лиценз по чл. 44, ал. 2 – 3 за съответното проектно хранилище.

(4) (Предишна ал. 3 – ДВ, бр. 80 от 2024 г.) Създаването на потребителски профил и на проектно хранилище е свободно и безплатно.

(5) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., предишна ал. 4, бр. 80 от 2024 г.) Министърът на електронното управление определя длъжностни лица, които административат хранилището.

(6) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г., предишна ал. 5, бр. 80 от 2024 г.) Достъп за запис в съществуващо проектно хранилище се предоставя по ред, определен от министъра на електронното управление.

(7) (Предишна ал. 6, изм. – ДВ, бр. 80 от 2024 г.) Копие от съдържанието на хранилището е достъпно и на интернет адрес "<https://github.com/government.bg>".

Работа с проектно хранилище

Чл. 60. (1) Изпълнителите по договори за изграждане и надграждане на софтуер използват проектни хранилища за ежедневна работа.

(2) (Изм. – ДВ, бр. 80 от 2024 г.) Лица извън администрацията и изпълнителите могат да предлагат подобрения в изходния код на софтуера в проектното хранилище.

(3) (Изм. – ДВ, бр. 80 от 2024 г.) Предложенията по ал. 2 подобрения се преглеждат от възложителя по конкретния договор в 30-дневен срок, след което ги приема или отказва мотивирано.

(4) (Изм. – ДВ, бр. 80 от 2024 г.) В хранилището приетите по ал. 3 предложения се добавят чрез функционалност за обединяване на промени на системата за контрол на версиите.

Раздел V

Портал за разработчици

Обхват

Чл. 61. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление изгражда и поддържа портал за разработчици на интернет адрес: dev.egov.bg.

(2) В портала за разработчици се поддържат:

1. библиотеки за достъп до регистри;
2. библиотеки, предоставящи обща функционалност;
3. документация на интерфейсите на регистрите и информационните системи в структуриран вид;
4. инструкции за интеграция за всеки регистър;
5. връзки към изходния код на библиотеки, регистри и други информационни системи.

Поддържане

Чл. 62. (1) При изготвяне на технически задания административните органи задължително включват изискване за добавяне и поддържане на съответните елементи в портала по чл. 61.

(2) Регистрацията в портала е свободна и безплатна.

(3) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление определя длъжностни лица, които администрират портала.

(4) Длъжностните лица по ал. 3 предоставят права на други длъжностни лица, определени от ръководителите на административните органи, за управление на ресурси, свързани със съответните администрации.

(5) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Порталът позволява подаване на предложения от страна на заинтересовани страни. Предложенията се приемат или отхвърлят от длъжностни лица, определени от министъра на електронното управление, които изпращат отговор или коментар на предложението.

Глава шеста "а"

(Нова – ДВ, бр. 80 от 2024 г.)

ИЗПОЛЗВАНЕ НА СПОДЕЛЕНИТЕ РЕСУРСИ НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

Заявление

Чл. 62а. (Нов – ДВ, бр. 80 от 2024 г.) (1) Използването на споделените ресурси на електронното управление за нуждите на административните органи се одобрява от министъра на електронното управление или от оправомощено от него длъжностно лице въз основа на заявление. Образецът на заявлението се утвърждава от министъра на електронното управление или от упълномощено от него длъжностно лице, публикуван на официалната интернет страница на Министерството на електронното управление.

(2) Заявлението по ал. 1 се подава при условията и по реда на чл. 32.

(3) Срокът за произнасяне по заявлението по ал. 1 е 15 дни.

Ред за заявяване на използването на споделените ресурси

Чл. 62б. (Нов – ДВ, бр. 80 от 2024 г.) Редът за заявяване на използването на споделените ресурси на електронното управление включва:

1. заявяване на необходимия ресурс;
2. проверка за допустимост и основателност на заявлението:
 - а) заявлението подадено ли е от административен орган или чрез оправомощено от него лице;
 - б) заявени ли са всички изискуеми обстоятелства;
3. при наличие на несъответствия се изпраща уведомление на заявителя с указания за отстраняването им в 5-дневен срок;
4. преглед и оценка на техническата възможност за осигуряване на споделените ресурси; при наличие на съответния ресурс и техническа възможност за предоставянето му министърът на електронното управление или оправомощено от него длъжностно лице издава заповед за предоставяне на ресурса и уведомява заявителя;

5. ако в резултат на оценяването на възможността за предоставяне на ресурси се установи, че няма техническа възможност за предоставянето им, министърът на електронното управление или оправомощено от него длъжностно лице писмено уведомява заявителя с отказ или с предложение за редуциране на искания обем ресурси;
6. прекратяване на използването на предоставените ресурси се извършва след писмено разпореждане на министъра на електронното управление или на оправомощено от него длъжностно лице по искане на ползвателя за отпаднала необходимост;
7. министърът на електронното управление или оправомощено от него длъжностно лице има право да разпреди прекратяване на ползването, когато административният орган – ползвател, на когото са предоставени ресурсите, със свои действия или бездействия поставя под риск целостта и интегритета на споделените ресурси;
8. с цел осигуряване на целесъобразно използване на споделения ресурс, в случай че се установи, че предоставен ресурс или части от него не се използват за повече от три месеца, министърът на електронното управление или оправомощено от него длъжностно лице има право служебно да намали капацитета на предоставяните ресурси, за което уведомява ползвателя.

Справки

Чл. 62в. (Нов – ДВ, бр. 80 от 2024 г.) На всяко тримесечие оправомощено от министъра на електронното управление длъжностно лице изготвя справка за използването на предоставените споделени ресурси на електронното управление, която се публикува на интернет страницата на Министерството на електронното управление.

Стандарти и ниво на качество на услугите

Чл. 62г. (Нов – ДВ, бр. 80 от 2024 г.) (1) Стандартите и нивото на качество на услугите, предоставяни от споделените ресурси, се описват в Каталог на услугите, публикуван на официалната интернет страница на Министерството на електронното управление.

(2) За използването на Единната електронна съобщителна мрежа като част от споделените ресурси на електронното управление следва да се спазват следните стандарти:

1. 10/100/1000 Mbps меден порт;
2. 1 Gbps оптичен или меден порт (SFP модул);
3. 10 Gbps оптичен порт.

Глава седма КОНТРОЛ

Орган за контрол

Чл. 63. (1) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление осъществява контрол по изпълнението на наредбата.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление ежегодно представя отчет за осъществения контрол пред Министерския съвет.

(3) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) Министърът на електронното управление периодично възлага извършване на проверки за съответствие на регистри с изискванията на тази наредба.

(4) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) При системно неспазване на предписанията на министъра на електронното управление от страна на първичен администратор на данни той изготвя доклад до Министерския съвет.

ДОПЪЛНИТЕЛНА РАЗПОРЕДБА

§ 1. По смисъла на тази наредба:

1. "Регистър" е структурирана база данни, чието предназначение е да съхранява и да бъде доверен автентичен източник на данни, за който съществува нормативно основание и нормативно определен ред за вписване, заличаване и/или удостоверяване на обстоятелства. При необходимост данните в регистъра подлежат на логическа обработка.
2. "Удостоверителна административна услуга" е административна услуга, в резултат на която се издава официален документ, удостоверяващ факти, обстоятелства, права, задължения или тяхната липса, представляващи законен интерес за физически или юридически лица или изискуеми от трето лице на валидно правно основание.
3. "Браузър" е софтуерно приложение, което дава възможност на потребителя да визуализира и достъпва текст, графика, музика, електронни препратки и други ресурси, разположени на интернет страници в интернет или в локална мрежа.
4. "Ползваемост" е качество на информационната система, осигуряващо на потребителите удобство и възможност да постигнат целите, за които ползват определен потребителски интерфейс, с достатъчна ефективност, ефикасност и удовлетвореност.
5. "Достъпност" е качество на информационната система, осигуряващо възможността на всички граждани, независимо от възрастта и физическите им възможности, да наблюдават, разбират, управляват и контактуват посредством потребителски интерфейс.
6. "Кохерентен кеш" е част от информационна система, която позволява четене на данни от буфер в оперативна памет, като гарантира тяхната актуалност спрямо оригиналния източник.
7. "Програмен интерфейс" е автоматизиран софтуерен слой или компонент, с който една информационна система предоставя онлайн достъп до своя функционалност, включително приемане или предаване на данни, на други информационни системи или софтуерни приложения.
8. "Централен компонент" е компонент от софтуерната архитектура, чрез който се осъществява комуникация между две системи.
9. "Анонимизиране" е процес по премахване на информация от документ, чрез която дадено лице може да бъде идентифицирано.
10. "Първични данни" са данни, които възникват за първи път в информационна система на първичен администратор на данни и които съответният първичен администратор съхранява по силата на закон.
11. "Система за документооборот" е всяка система, която се използва за вътрешен оборот на електронни документи в администрациите съгласно чл. 42 ЗЕУ и/или за обмен на електронни документи между администрациите.
12. "EUPL (European Union Public License)" е свободен лиценз на Европейската комисия, който може да бъде намерен на следния интернет адрес: https://joinup.ec.europa.eu/community/eupl/og_page/european-union-public-licence-eupl-v11.
13. "GPL (General Public License) 3.0" е свободен лиценз на Фондацията за свободен софтуер (FSF), който може да бъде намерен на следния интернет адрес: <https://www.gnu.org/licenses/gpl-3.0.en.html>.
14. "LGPL (Lesser General Public License)" е свободен лиценз на Фондацията за свободен софтуер (FSF), който може да бъде намерен на следния интернет адрес: <https://www.gnu.org/licenses/lgpl-3.0.en.html>.
15. "AGPL (Affero General Public License)" е свободен лиценз на Фондацията за свободен софтуер (FSF), който може да бъде намерен на следния интернет адрес: <https://www.gnu.org/licenses/agpl-3.0.en.html>.
16. "Apache License 2.0" е свободен лиценз на Фондацията "Апачи софтуер", който може да бъде намерен на следния интернет адрес: <https://www.apache.org/licenses/LICENSE-2.0>.

17. "New BSD license" е свободен лиценз на Калифорнийския университет, Бъркли, който може да бъде намерен на следния интернет адрес: <https://opensource.org/licenses/BSD-3-Clause>.
18. "MIT License" е свободен лиценз на Масачузетския технологичен университет, който може да бъде намерен на следния интернет адрес: <https://opensource.org/licenses/MIT>.
19. "Mozilla Public License 2.0" е свободен лиценз на Фондация "Мозила", който може да бъде намерен на следния интернет адрес: <https://www.mozilla.org/en-US/MPL/2.0/>.
20. (Нова – ДВ, бр. 66 от 2018 г., в сила от 10.08.2018 г.) "Въвеждането в продукционен режим на националната схема за електронна идентификация" е датата на издаване на първото удостоверение за електронна идентичност по Закона за електронната идентификация.
21. (Нова – ДВ, бр. 66 от 2018 г., в сила от 10.08.2018 г., изм., бр. 80 от 2024 г.) "Уникален идентификатор" е единният граждански номер, личният номер за чужденец, личният номер на граждани на Европейския съюз и на членовете на техните семейства, които не са граждани на Европейския съюз, единният идентификационен код за търговците и клоновете на чуждестранните търговци и кодът по БУЛСТАТ за лицата, подлежащи на вписване в регистър БУЛСТАТ.
22. (Нова – ДВ, бр. 66 от 2018 г., в сила от 10.08.2018 г., изм., бр. 47 от 2022 г., в сила от 24.06.2022 г.) "Система за електронна автентикация" е хоризонтална система, чрез която се идентифицират лицата и информационните системи в електронния свят, създадена и поддържана от Министерството на електронното управление.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 2. Наредбата се приема на основание чл. 7г, ал. 6, чл. 12, ал. 4 и чл. 43, ал. 2 от Закона за електронното управление.

§ 3. (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) В срок до 1 юни 2018 г. за идентифициране на информационна система, освен сертификат, регистриран в Интегрираната информационна система за държавната администрация, може да се използват и сертификат или ключ, издаден от министъра на вътрешните работи или от министъра на електронното управление, както и сървърен SSL сертификат.

§ 4. Задължението за вход по реда на Закона за електронната идентификация в системи за електронен документооборот по чл. 34, ал. 2 от наредбата влиза в сила от 1 януари 2019 г.

§ 5. (Изм. – ДВ, бр. 66 от 2018 г., в сила от 10.08.2018 г.) (1) В срок една година след въвеждането в продукционен режим на националната схема за електронна идентификация по Закона за електронната идентификация за идентификация на физически лица, освен по реда на Закона за електронната идентификация и чрез други методи, определени със закон, може да се прилага и прочитане на уникален идентификатор от квалифициран електронен подпис.

(2) (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) В срок три години след въвеждането в продукционен режим на националната схема по ал. 1 за електронна идентификация на физически лица при заявяването на електронни административни услуги може да се използва и персоналният идентификационен код, издаван от Националната агенция за приходите или Националния осигурителен институт, както и уникалният код за достъп, издаван от Националната здравноосигурителна каса, след интеграцията им със системата за електронна автентикация на Министерството на електронното управление.

§ 6. Задължението за използване на електронен документооборот по чл. 32, ал. 1 и 2 от наредбата влиза в сила от 1 ноември 2018 г., като до влизането му в сила администрациите не поставят печат на документите на хартиен носител, които обменят.

§ 7. (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) В срок до 1 септември 2017 г. министърът на електронното управление публикува препоръките, правилата и насоките съответно по чл. 39, 40 и 43.

§ 8. (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) В срок до 1 януари 2018 г. министърът на електронното управление определя техническия протокол по чл. 18.

§ 9. До изграждането на хранилището по чл. 58 се използва хранилището, което се намира на [GitHub.com/governmentbg](https://github.com/governmentbg).

§ 10. (Изм. – ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.) До изграждането на системите и регистрите по глава шеста, раздели I, II и III ръководителите на административните органи изпращат съответните данни по ред, определен от министъра на електронното управление.

§ 11. При изготвянето на технически задания за изграждане или надграждане на информационни системи администрациите са длъжни да включват съответно изискванията на наредбата без оглед на момента на влизането им в сила.

§ 12. При консолидирано водене на регистри по реда на чл. 13 се осигурява достъп за трети страни по досегашния ред за срок най-малко 24 месеца.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

към Постановление № 164 на Министерския съвет от 6 август 2018 г. за изменение на Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги
(ДВ, бр. 66 от 2018 г., в сила от 10.08.2018 г.)

§ 3. Идентификацията на физически лица, извършена чрез прочитане на уникален идентификатор от квалифициран електронен подпис до влизането в сила на постановлението, се приема за валидно извършена.

.....

ПОСТАНОВЛЕНИЕ № 134

на Министерския съвет от 20 юни 2022 г. за изменение и допълнение на нормативни актове на Министерския съвет
(ДВ, бр. 47 от 2022 г., в сила от 24.06.2022 г.)

§ 1. В Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, приета с Постановление № 3 на Министерския съвет от 2017 г. (обн., ДВ, бр. 5 от 2017 г.; изм. и доп., бр. 66 от 2018 г. и бр. 4 от 2020 г.), навсякъде думите "Председателят на Държавна агенция "Електронно управление", "председателят на Държавна агенция "Електронно управление", "председателя на Държавна агенция "Електронно управление" и "Държавна агенция "Електронно управление" се заменят съответно с "Министърът на електронното управление", "министърът на електронното управление", "министъра на електронното управление" и "Министерството на електронното управление".

.....

Приложение				№			1
към		чл.		38,	ал.		3
(Изм.	–	ДВ,	бр.	47	от	2022	г.,
в		сила	от		24.06.2022		г.,
бр. 80 от 2024 г.)							

[Възложител]
ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ
за
[Име на проект]

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ
 - 1.1. Използвани акроними
 - 1.2. Технологични дефиниции
 - 1.3. Дефиниции за нива на електронизация на услугите
2. ВЪВЕДЕНИЕ
 - 2.1. Цел на документа
 - 2.2. За възложителя – функции и структура
 - 2.3. За проекта
 - 2.4. Нормативна рамка
3. ЦЕЛИ, ОБХВАТ И ОЧАКВАНИ РЕЗУЛТАТИ ОТ ИЗПЪЛНЕНИЕ НА ПРОЕКТА
 - 3.1. Общи и специфични цели на проекта
 - 3.2. Обхват на проекта
 - 3.3. Целеви групи
 - 3.4. Очаквани резултати
 - 3.5. Период на изпълнение
4. ТЕКУЩО СЪСТОЯНИЕ
5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА
 - 5.1. Общи изисквания към изпълнението на обществената поръчка
 - 5.2. Общи организационни принципи
 - 5.3. Управление на проекта
 - 5.4. Управление на риска
6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА
 - 6.1. Анализ на данните и изискванията
 - 6.1.1. Специфични изисквания към етапите на бизнес анализа при разработка, надграждане или внедряване на информационна система
 - 6.1.2. Специфични изисквания при оптимизиране на процесите по заявяване на електронни услуги и електронни административни услуги (съгл. § 1, т. 2 от ЗЕУ) в зависимост от заявителя
 - 6.1.3. Изисквания за оптимизиране на процесите по подаване на декларации, изискуеми в съответствие с нормативната уредба и вътрешните правила
 - 6.1.4. Изисквания към регистрите и предоставянето на административните услуги
 - 6.2. Изготвяне на системен проект
 - 6.3. Разработване на софтуерното решение
 - 6.4. Тестване
 - 6.5. Внедряване
 - 6.6. Обучение
 - 6.7. Гаранционна поддръжка
 - 6.7.1. Обхват на дейностите по гаранционна поддръжка
 - 6.7.2. Управление на инциденти
 - 6.7.3. Управление на проблеми
 - 6.7.4. Управление на качеството при отстраняване на инциденти и проблеми. Параметри на качеството
 - 6.7.5. Минимални изисквания към параметрите на качеството
 - 6.7.6. Управлението на промените

- 7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ
 - 7.1. Функционални изисквания към информационната система
 - 7.1.1. Интеграция с външни информационни системи
 - 7.1.2. Използване на интеграционен слой на електронното управление
 - 7.1.3. Технически изисквания към интерфейсите
 - 7.1.4. Електронна идентификация на потребителите
 - 7.1.5. Отворени данни
 - 7.1.6. Формиране на изгледи
 - 7.1.7. Администриране на Системата
 - 7.2. Нефункционални изисквания към информационната система
 - 7.2.1. Авторски права и изходен код
 - 7.2.2. Системна и приложна архитектура
 - 7.2.3. Повторно използване (преизползване) на ресурси и готови разработки
 - 7.2.4. Изграждане и поддръжка на множество среди
 - 7.2.5. Процес на разработка, тестване и разгръщане
 - 7.2.6. Бързодействие и мащабируемост
 - 7.2.7. Информационна сигурност и интегритет на данните
 - 7.2.8. Използваемост
 - 7.2.9. Системен журнал
 - 7.2.10. Дизайн на бази данни и взаимодействие с тях
 - 7.2.11. Изисквания по отношение на киберсигурност в съответствие с чл. 12, ал. 1 от НМИМИС
- 8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА
 - 8.1. Дейност 1 [Наименование на дейността]
 - 8.1.1. Описание на дейността
 - 8.1.2. Изисквания към изпълнение на дейността
 - 8.1.3. Очаквани резултати
 - 8.2. Дейност 2 [Наименование на дейността]
 - 8.2.1. Описание на дейността
 - 8.2.2. Изисквания към изпълнение на дейността
 - 8.2.3. Очаквани резултати
 - 8.3. Дейност 3 [Наименование на дейността]
 - 8.3.1. Описание на дейността
 - 8.3.2. Изисквания към изпълнение на дейността
 - 8.3.3. Очаквани резултати
 - 8.4. Дейност 4 [Наименование на дейността]
 - 8.4.1. Описание на дейността
 - 8.4.2. Изисквания към изпълнение на дейността
 - 8.4.3. Очаквани резултати
 - 8.5. Дейност 5 [Наименование на дейността]
 - 8.5.1. Описание на дейността
 - 8.5.2. Изисквания към изпълнение на дейността
 - 8.5.3. Очаквани резултати
- 9. ДОКУМЕНТАЦИЯ
 - 9.1. Изисквания към документацията
 - 9.2. Прозрачност и отчетност
 - 9.3. Системен проект
 - 9.4. Техническа документация
 - 9.5. Протоколи
 - 9.6. Комуникация и доклади
 - 9.6.1. Встъпителен доклад
 - 9.6.2. Междинни доклади
 - 9.6.3. Окончателен доклад
- 10. РЕЗУЛТАТИ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

Използвани акроними

Акроним	Описание
АИС	Автоматизирана информационна система
АМС	Администрация на Министерския съвет
АО	Административен орган
АОП	Агенция по обществени поръчки
АПК	Административнопроцесуален кодекс
БУЛСТАТ	Регистър Булстат
МЕУ	Министерство на електронното управление
ЗДОИ	Закон за достъп до обществена информация
ЗЕУ	Закон за електронното управление
ИТ	Информационни технологии
КАО	Комплексно административно обслужване
ТР	Търговски регистър
ДХЧО	Държавен хибриден частен облак
ЦАИС	Централизирана автоматизирана информационна система
SDK	Software development kit
API	Application programming interface/Приложно програмен интерфейс

Технологични дефиниции

Термин	Описание
Виртуална комуникационна инфраструктура	Инфраструктура, която на база съществуваща физическа свързаност, предоставена от МЕУ, 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 на 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.

Наличност на Системата в проценти	Процентът на договорените часове, за които компонент или услуга е достъпна за определен период от време.
Работни дни	От понеделник до петък без националните и официалните празници.
Работни часове (Работно време)	08:00-20:00 всеки работен ден
Инцидент	Инцидент е всяко намаляване на качеството или недостъпност на предоставяна услуга и/или непланираното ѝ прекъсване, както и неизправност на елемент от инфраструктурната конфигурация
Продължително прекъсване	Прекъсване на услугата за повече от четири (4) работни часа
Планирана недостъпност	Планирано прекъсване на една или повече услуги.
Нестъпност	Неспособността на услуга или част от услуга да осигури нормалното обслужване
Непланирана недостъпност	Неочаквано прекъсване на една или повече услуги или значителна деградация на качеството на предлаганата услуга.
Проблем	Проблем е съвкупност от повтарящи се идентични събития или инциденти, които водят до периодично влошаване на дадена услуга, липсата ѝ или неточност в дадена процедура или функционално звено

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 на услуги изцяло по електронен път, включително електронно подаване на данни и документи, електронна обработка на формуляри и електронна идентификация на потребителите, освен ако със закон се допуска предоставяне на електронна административна услуга без идентификация.
Ниво 4	Извършване на услуги от ниво 3, за които е осигурена възможност за електронно връчване и електронно плащане, ако за получаването на електронна административна услуга се дължат такси.

2. ВЪВЕДЕНИЕ

2.1. Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на обществена поръчка с предмет: *[опишете предмета на поръчката]*.

В настоящата техническа спецификация са описани и изискванията към проектната организация, документацията и отчетността.

Съдържанието на настоящата техническа спецификация е задължително за прилагане от всички лица по чл.1, ал.1 и ал. 2 от ЗЕУ, публичните и секторните възложители по Закона за обществените поръчки, които са публични предприятия по смисъла на Закона за публичните предприятия, като в същото може да бъде добавян текст в зависимост от специфичните нужди на разработваната информационна система, но не може да бъде изтривано настоящото съдържание.

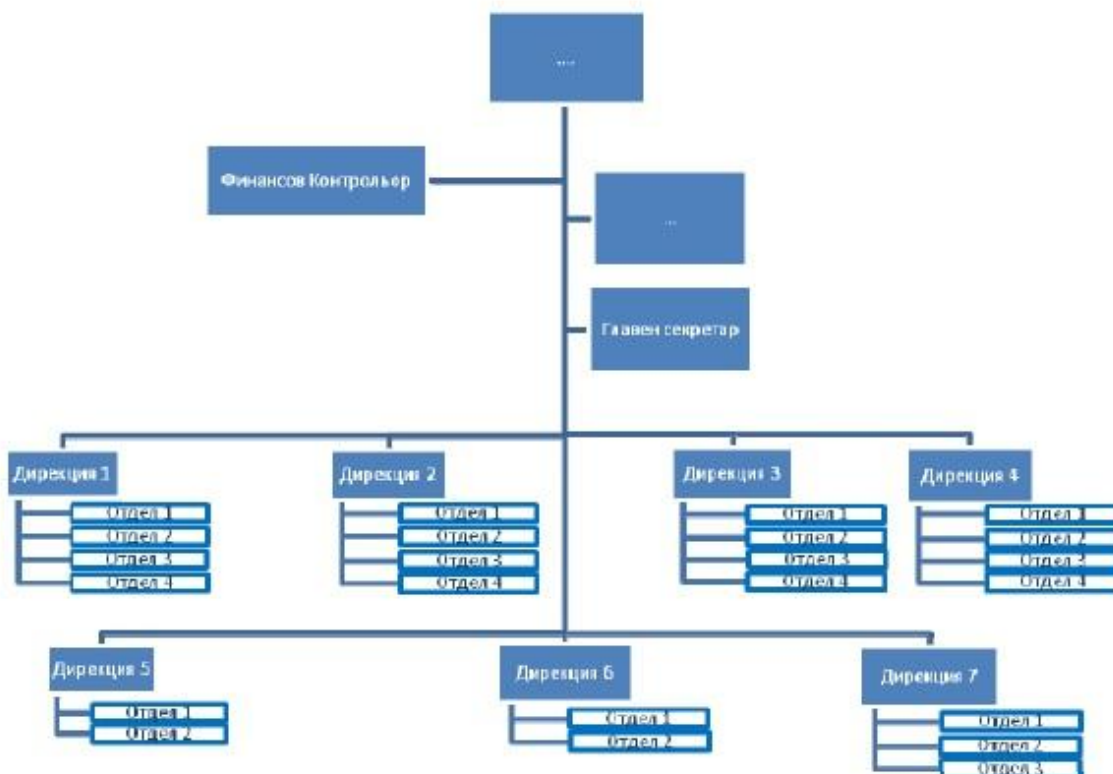
2.2. За възложителя – функции и структура



Опишете накратко функциите на Вашата администрация.

Изтрийте тази текстова кутия при финализиране на документа.

Структурата на *[възложителя]* е представена във Фигура 1:



Фигура 1. Структура на *[възложителя]*

2.3. За проекта



Кратка информация за проекта

Изтрийте тази текстова кутия при финализиране на документа.

2.4. Нормативна рамка

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

- Закон за електронното управление (ЗЕУ);
- Закон за киберсигурност (ЗК);
- Закон за електронната идентификация (ЗЕИ);
- Наредба за общите изисквания към информационните системи, регистри и електронни административни услуги (НОИИСРЕАУ);
- Наредба за минималните изисквания за мрежова и информационна сигурност (НМИМИС);
- Актуализирана стратегия за електронното управление;
- Архитектура на електронното управление
- [Документ 2]

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

3.1. Общи и специфични цели на проекта

Проектът е насочен към *[подробно описание на общата цел на проекта]*.

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

- [Специфична цел 1]
- [Специфична цел 2]
- [Специфична цел 3]
- [Специфична цел 4]
- [Специфична цел 5]

3.2. Обхват на проекта

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

- Дейност 1 *[Наименование на дейността]*
- Дейност 2 *[Наименование на дейността]*
- Дейност 3 *[Наименование на дейността]*
- Дейност 4 *[Наименование на дейността]*
- Дейност 5 *[Наименование на дейността]*

Подробна информация за конкретните дейности по проекта е публично достъпна на адрес

3.3. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

- [Целева група 1];
- [Целева група 2];
- [Целева група 3].



Вашата администрация задължително присъства в списъка с целеви групи. Други целеви групи могат да бъдат други организации, например държавни администрации, крайни потребители на административни услуги – гражданите и бизнесът, както и други лица, осъществяващи публични функции.



Опишете какви резултати очаквате да бъдат постигнати с реализирането на проекта.

Изтрийте тази текстова кутия при финализиране на документа.

Изтрийте тази текстова кутия при финализиране на документа.

3.4. Очаквани резултати

Очакваните резултати от изпълнението на настоящата поръчка са:

- [Резултат 1];
- [Резултат 2];
- [Резултат 3].

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



Опишете текущото състояние на Вашата администрация и бизнес процесите, които имат отношение към предмета на процедурата.

Изтрийте тази текстова кутия при финализиране на документа.

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

5.1. Общи изисквания към изпълнението на обществената поръчка

Обществената поръчка се изпълнява в рамките на *[Наименование на проекта/дейността]*, финансиран по *[Източник на финансиране]*. Изпълнителят следва да спазва всички нормативни изисквания по отношение на дейността на *[бенефициента]* и електронното управление в Република България.

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 проекта¹

[Моля, изтрийте ненужното!] Участниците трябва да предложат методология за управление на проекта, която смятат да приложат, като се изтъкнат ползите ѝ за успешното изпълнение на проекта. Предложената методология трябва да съответства на най-добрите световни практики и препоръки (например Project Management Body of Knowledge (PMBOK) Guide, PRINCE2, Agile/ SCRUM/ Kanban, RUP и др. еквивалентни).

Участникът следва да организира изпълнението на дейностите си съгласно принципите на избрана от него Методология за управление на ИТ проекти и да предложи план-график за изпълнение на проекта за всяка дейност и поддейност.

[Моля, изтрийте ненужното!] Възложителят изисква методология за управление на проекта, която участниците трябва да приложат и която съответства на най-добрите практики и препоръки, а именно *[Моля, довършете изречението!]*.

Дейностите по управление на проекта трябва да включват като минимум управление на реализацията на целия обхват на настоящата обществена поръчка и постигане на очакваните резултати, както и разпределението на предложените

¹ Под „проект“ следва да се разбира предметът на настоящата обществена поръчка

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;
- 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;
- Ненавременен 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;
- Неинформирание 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

- *[Моля, изтрийте ненужното!]* Разработка, надграждане и внедряване на публични електронни административни услуги;
- *[Моля, изтрийте ненужното!]* Разработка, надграждане и внедряване на вътрешноадминистративни услуги;
- *[Моля, изтрийте ненужното!]* Разработка на нови функционалности на Системата и надграждане на съществуващи;
- *[Моля, изтрийте ненужното]* Разработка на нови регистри и надграждане на съществуващи. Актуализиране на модела на данните и системата за управление на базата данни (СУБД).
- 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 вътрешни електронно административни услуги за нуждите на комплексното административно обслужване чрез служебен онлайн интерфейс.

6.1.1. Специфични изисквания към етапите на бизнес анализа при разработка, надграждане или внедряване на информационна система

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;

- Необходимо е да бъде направен анализ на текущото състояние на данните, които ще се обработват, по отношение на тяхната изчерпателност, пълнота и качество, да се направи оценка на възможността за въвеждане на данни и обстоятелства в регистри, съгласно изискванията на нормативната уредба. Да се предложи модел на данните, съдържащ описание на основните таблици и схематично представяне на връзките между тях;

- В процеса на анализа трябва да се разгледа възможността обменът на данни да се основава на общи стандарти, т.е. условия за използване, формат на данните, машинна четимост, метаданни, споделени речници/таксономии, честота, детайлност и задължителни атрибути. Задължителното прилагане би гарантирало изпълнението на изискванията за повторни потребители и доставчици на данни.

- Трябва да бъде направен анализ, оценка и описание на работните процеси, заложи в нормативната уредба, да бъде предложена организационна архитектура на базата, на която да бъдат разработени и оптимизирани основните функционалности на Системата.

- Трябва да бъдат предвидени периодични продуктови тествания по време на разработката и внедряването на Системата, с извадка (фокус-група) от бъдещите потребители на Системата, чрез които да се изпита и оцени използваемостта на услугите и потребителските интерфейси, както и за да бъдат отстранени затруднения и несъответствия със спецификацията;

- 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 базата 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 структуриран електронен формуляр, върху който потребителите трябва да се подписват 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 администратират 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;

6.1.2. Специфични изисквания при оптимизиране на процесите по заявяване на електронни услуги и електронни административни услуги (съгл. §1, т.2 от ЗЕУ) в зависимост от заявителя

▪ Предвидените за разработка и внедряване електронни административни услуги трябва да бъдат регистрирани предварително в Регистъра на услугите към Административния регистър (съгласно чл. 61 от Закона за администрацията). 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;

▪ При разработката на информационна система, чрез която се предоставят ЕАУ, да се предвиди изцяло автоматизираното им предоставяне, като се определи задължителното минимално ниво на електронизация на ЕАУ, съгласно т. 1.3 от техническата спецификация, както и нивото на осигуреност на средствата за електронна идентификация при заявяване на ЕАУ, определено съгласно Методика за определяне от лицата по чл. 1, ал. 1 и 2 от ЗЕУ на средствата за електронна идентификация, които се използват при заявяване на ЕАУ, и тяхното ниво на осигуреност, и получаване на резултата от нея.

▪ При анализа трябва да се има предвид, ако АО предоставя ЕАУ от ниво 4, изискваща такса за плащане, тя е с намалена такса спрямо таксата за присъствено заявяване и предоставяне, ако при прилагането на методиката за определяне на разходоориентиран размер на таксите по чл. 7а на Закона за ограничаване на административното регулиране и административния контрол върху стопанската дейност се установи различен размер на разходите, съгласно чл.10а, ал 2 от ЗЕУ.

▪ Трябва да се разработят информативни текстове за всяка услуга, които включват като минимум:

- условия за предоставяне на услугата;
- срокове за предоставяне на услугата;
- такси за заявяване и съответно предоставяне на услугата;
- начини за получаване на услугата;
- резултат от предоставяне на услугата;
- отказ от предоставяне на услугата.

- Информативните текстове за всяка услуга трябва да бъдат достъпни за потребителите още като първа стъпка от заявяването на услуга;
- Тарифирането на услугите трябва да бъде реализирано така, че Системата да съхранява всички версии на тарифите за услуги (от дата до дата) и да прилага съответната тарифа в зависимост от момента, в който е заявена дадена услуга;
- Трябва да бъде оптимизиран потребителският път от влизане на сайта до заявяване и получаване на услуга и пътят от регистрация на нов потребител до заявяване и получаване на услуга;
- 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.
- Съгласно действащата нормативна уредба допустимите заявители на електронни административни услуги могат да бъдат разделени в няколко групи, като процесите по заявяване на ЕАУ и необходимите процеси по установяване на допустимостта на заявлението зависят от множество фактори. Трябва да бъде обърнато специално внимание на спецификите в процесите в зависимост от качеството, в което действа заявителят, за да се постигне максимална оптимизация на процеса, като същевременно се защити сигурността на търговския и гражданския оборот.
- Предоставянето на ЕАУ от административните органи на гражданите и бизнеса да се извършва през Портала на електронното управление чрез хоризонталната система за е-форми, като се използва Единният модел за заявяване, заплащане и предоставяне на ЕАУ.

В приложената диаграма са показани възможни разлики в бизнес процесите в зависимост от качеството, в което действа заявител на ЕАУ:

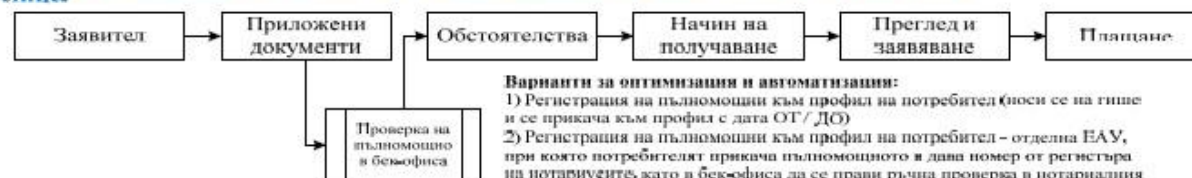
Процес по заявяване „в лично качество“



Процес по заявяване на услуга като законен представител на юридическо лице



Процес по заявяване на услуга като пълномощник на физическо или юридическо лице

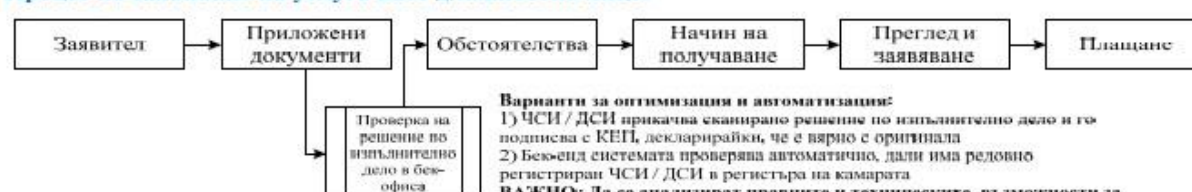


Варианти за оптимизация и автоматизация:

- 1) Регистрация на пълномощник към профил на потребител (носи се на гише и се прикача към профил с дата ОТ / ДО)
- 2) Регистрация на пълномощник към профил на потребител – отделна ЕАУ, при която потребителят прикача пълномощното и дава номер от регистъра на нотариусите, като в бек-офиса да се прави ръчна проверка в нотариалния регистър на пълномощните „Единство“, преди да се активира

ВАЖНО: Да се анализират правните и техническите възможности за осигуряване на служебен достъп до регистъра на пълномощните, поден от нотариалната камара!

Процес по заявяване на услуга като длъжностно лице



Варианти за оптимизация и автоматизация:

- 1) ЧСИ / ДСИ прикачва сканирано решение по изпълнително дело и го подписва с КЕП, декларирайки, че е вярно с оригинала
- 2) Бекенд системата проверява автоматично, дали има редовно регистриран ЧСИ / ДСИ в регистъра на камарата

ВАЖНО: Да се анализират правните и техническите възможности за осигуряване на служебен достъп до регистъра на пълномощните, поден от нотариалната камара!

В приложената таблица са представени спецификите и разликите в бизнес процесите в зависимост от качеството, в което действа заявител на ЕАУ, които трябва да бъдат отразени при реализацията на Системата:

Вид заявител	Особености	Специфични процеси
Физическо лице за собствени нужди	Заявява ЕАУ за лични нужди от свое име. Това е най-простият за реализиране случай	Услугата може да бъде предоставена, след като са изпълнени нуждите за идентификация, ако има такива - електронна идентификация по смисъла на ЗЕИ или ЕГН, извлечено от КЕП в преходния период, както и три имена или анонимно.
Законен представител на юридическо лице	Заявява ЕАУ, за да обслужи нужди на юридическо лице, на което е законен представител (т.е. заявителят е вписан като представляващ юридическото лице в съответен регистър)	Услугата може да бъде предоставена, след като са изпълнени нуждите за идентификация - електронна идентификация по смисъла на ЗЕИ или ЕГН, извлечено от КЕП в преходния период, както и автоматична проверка за представителна власт в ТР/ БУЛСТАТ/ ЦРЮЛНЦ.
Пълномощник на ФЛ или ЮЛ	Заявява ЕАУ, за да обслужи нужди на физическо или юридическо лице, което го е упълномощило (т.е. заявителят трябва да разполага с пълномощно, което му дава необходимия обем и обхват на представителна власт, за заявяване и/или получаване на съответната услуга)	Услугата може да бъде предоставена само след проверка на представителната власт в Регистъра с пълномощни на Нотариалната камара, чрез проверка в Регистъра на овластяванията по смисъла на ЗЕИ или при създадена възможност за регистриране на пълномощни към профила на потребителя или за заявяване на услугата. Пълномощник може да бъде и посредник за предоставяне на ЕАУ по реда на ЗЕУ, в т.ч. Центрове за комплексно административно обслужване.
Длъжностно лице (ЧСИ / ДСИ)	Заявява ЕАУ, за да изпълни определени свои задължения като длъжностно лице спрямо друго физическо или юридическо лице, за което следва да има съответен правен интерес.	Услугата може да бъде предоставена само след проверка на длъжностното лице в съответния регистър (ЧСИ/ ДСИ) и на правния интерес чрез изискване за декларирането му чрез изрична декларация, подписана с КЕП, и прилагане на копие от решение по изпълнително дело.

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

- Системата трябва да поддържа номенклатура с редактируеми шаблони на декларации, които да бъдат достъпни за актуализация за администраторите на Системата; Трябва да се поддържа история на версиите на шаблоните и да няма възможност за перманентно премахване/изтриване на шаблони, а само смяна на статуса им и публикуване на нова версия;

- Ако даден бизнес процес изисква подаване на декларация от страна на заявител на услуга, при достигане на съответната стъпка от процеса Системата трябва:

- да попълва автоматично всички персонални данни на заявителя в електронна форма, генерирана на база на съответния шаблон на декларация;
- да дава възможност на потребителя за избор на съответните обстоятелства, които може да декларира (ако шаблонът на декларацията предвижда възможност за деклариране на опционален набор от предефинирани обстоятелства);
- да изисква потвърждение на обстоятелствата от страна на потребителя;
- в случай че декларацията трябва да се попълни от лице, различно от заявителя, тя да може да се прикачи като електронно подписан документ или по електронен път да бъде отправяна покана към декларатора за електронно подписване.

▪ Всяка попълнена електронна декларация трябва да се прикачи автоматично от Системата към заявлението и да бъде подписана заедно с него от потребителя с електронен подпис, освен в случаите, когато заявителят и деклараторът са различни лица и декларацията е подписана отделно от декларатора.

6.1.4. Изисквания към регистрите и предоставянето на административните услуги

▪ Всяка удостоверителна административна услуга в обхвата на Системата трябва да бъде достъпна като вътрешноадминистративна електронна услуга чрез уеб услуга, като комуникацията се подписва с електронен печат на институцията и с електронен времеви печат по смисъла на Регламент (ЕС) 910/2014;

▪ Всяка услуга, за която се допуска представителна власт, трябва да бъде интегрирана с Регистъра на овластяванията по смисъла на Закона за електронната идентификация;

▪ Системата не трябва да съхранява данни, на които възложителят не е първичен администратор, в случай че данните могат да бъдат извлечени в реално време от регистър на съответния първичен администратор при възможност чрез интеграционната шина за обмен на справочна и удостоверителна информация.

▪ Всички електронни административни услуги, предоставяни от административните органи на гражданите и бизнеса, трябва да се заявяват през Портал за електронно управление.

▪ При предоставянето на ЕАУ е необходимо Изпълнителят да осъществи интеграция с хоризонталните системи на електронното управление.

6.2. 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 техническата спецификация;

▪ 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 [X] работни дни.

6.3. 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 настоящата техническа спецификация 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.

6.4. 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.

6.5. Внедряване

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

6.6. Обучение

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

- *[Потребителска група 1];*
- *[Потребителска група 2];*
- *[Потребителска група 3].*

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка *[включват се само тези точки, за които Възложителят няма възможност да осигури изброените ресурси]*:

- Необходимия хардуер;
- Необходимия софтуер;
- Зала/Зали за провеждане на обученията;
- Учебни материали;
- Лектори.

6.7. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от минимум *[X]* месеца след въвеждане 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, заложи в системния проект.

Приоритетите на инцидентите и проблемите се определят от Възложителя в зависимост от влиянието им върху работата на администрацията. Редът на отстраняването им се определя в зависимост от техния приоритет.

6.7.1. Обхват на дейностите по гаранционна поддръжка

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

Дейностите по гаранционна поддръжка трябва да включват следния минимален обхват:

- Извършване на диагностика с цел осигуряване на правилното и безпроблемно функциониране на Системата;
- Регистриране на инцидент в Система за управление на инциденти и проблеми;
- Отстраняване на дефектите, открити в софтуерните и/или хардуерните модули;
- Възстановяването на работоспособността на Системата при евентуален срив;
- Предоставяне на консултации за идентифициране на проблеми в конфигурацията на ИТ средата (операционна система, база данни, middleware, хардуер и мрежи);
- Регулярен мониторинг на неразрешените инциденти, дефиниране на проблеми и оценка на ефектите върху договорените параметри на качеството за наличност и достъпност на Системата;
- Пълно документиране на разрешените инциденти, включително предприетите стъпки за разрешаването им, точното им класифициране, обратна връзка със засегнатите потребители относно предложеното решение, общо изразходвано време за разрешаване;
- Актуализация на документацията 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.

За целите на дейността е необходимо да бъдат изготвени от Изпълнителя и одобрени и подписани от Възложителя:

- Споразумение за нивото на предоставяните услуги към потребителите на информационни ресурси на АО (SLApm), в които са определени приоритетите за спешно обслужване;

- Параметрите на качество на обслужване на Системата, съобразени с минималните изисквания към параметрите на качеството от т. 6.7.5;
- Комуникационни, анализаторски и документационни средства, с които функционалните звена идентифицират, анализират, проследяват и документират възникването и отстраняването на неработоспособността на информационната система.

6.7.2. Управление на инциденти (incident management)

С цел осигуряване на работоспособността на Системата и повишаване на качеството на обслужване на потребителите ѝ в етапа на нейната експлоатация, Изпълнителят трябва да разработи процедури за бързо и ефективно регистриране на възникнали инциденти и безпроблемно им отстраняване.

Чрез процедурата за управление на инциденти се подпомага и координира работата на въвлечените в тази дейност функционални звена, които изпълняват следните задачи:

1-во ниво на поддръжка – за изпълнение на тези дейности се сформира се екип от експерти на Възложителя или дейността се поема от екип на Изпълнителя. Задачите на екипа са да извършва дейности по наблюдение на Системата, регистриране, описание и обслужване на инциденти с цел улесняване идентифицирането на причините за възникване, първоначален анализ и класифициране на инциденти, ескалиране на заявки към 2-ро ниво поддръжка, документиране на дейностите и изготвяне на доклади.

2-ро ниво на поддръжка – екипът се сформира от експерти на Изпълнителя или от експерти на Възложителя и Изпълнителя, които разглеждат, анализират и отстраняват всички възникнали инциденти при спазване на процедурата. Екипът изпълнява следните задачи: обслужване на ескалираните от 1-во ниво на поддръжка инциденти, анализиране и класифициране на инциденти, разследване и диагностика на инцидента и установяване на средствата и каналите за разрешаване, разрешаване на инцидента и възстановяване на оперативността на всички засегнати компоненти, създаване на база данни за начина на разрешаване на инцидентите, съдържаща информация както за временните решения (work around), така и за искания за промени;

3-то ниво на поддръжка – екипът се сформира от експерти на Изпълнителя, които разрешават инцидент, ескалиран от екипа на 2-ро ниво на поддръжка, осигуряват безпроблемното функциониране на Системата, проактивно изследват инцидент с цел откриване на конкретната причина за възникването му, правят предложения за промени в компонентите, свързани с решаването на регистрирани проблеми, предоставят информация за процеса по управление на проблемите (Problem Management) относно взимане на мерки за предотвратяване повторемостта на инцидентите.

Процесът на управление на инциденти се осъществява чрез използване на Система за управление на заявки (Service/ Help Desk), собственост на Възложителя или Изпълнителя, която гарантира разпознаването им, тяхната проследимост и причините за възникването им, позволява документиране, комуникиране и одобрение по идентификация, разследване и отстраняване на причини за възникване на инциденти и проблеми.

6.7.3. Управление на проблеми (УП) (problem management)

В етапа на гаранционна поддръжка се включва процесът по управление на проблеми, целта на който е да минимизира и/или елиминира влиянието на инцидентите, причинени от грешки, възникнали в компонентите на системите, платформите, функционалните звена и/или процесите, имащи пряко или косвено отношение към влошаване или невъзможност за предоставяне на услугите към крайните потребители. При УП екипът от експерти на Изпълнителя трябва:

- да се фокусира върху идентифицирането на причините за възникване на инциденти (root-cause analysis), повторемостта на идентичните събития и инциденти, които водят до появата и съществуването на грешки.

- да извършва всички необходими дейности за диагностициране и анализиране на причините за възникване на инцидентите и да определя начините и методите за разрешаване на проблемите, да дефинира, прилага и да носи пряка отговорност за прилагането на подходящи контролни процедури (Change Management/ Release Management) с цел безпроблемно и качествено имплементиране на одобреното постоянно или временно (work around) решение.
- да поддържа база данни - инструмент за работа с нея, в която се вписват всички проблеми и съответните им решения (Knowledge Management and Known Error Data Base).
- да обхване двата основни процеса – реактивно и проактивно управление на проблемите, който е част от процеса на непрекъснато подобряване на услугите (Continuous Service Improvement).

6.7.4. Управление на качеството при отстраняване на инциденти и проблеми. Параметри на качеството.

Чрез гаранционната поддръжка Изпълнителят трябва да осигури гарантиране на работоспособността, на мрежовата и информационната сигурност, да поддържа непрекъснатост на работата на Системата, с което се обезпечава неприкосновеността и сигурността на обработваната информация.

Параметрите на качеството на услугите, които Изпълнителят предлага в етапа на гаранционна поддръжка, се изпълняват съгласно споразумение за нивото на предоставяните услуги към потребителите на АО (SLApm).

6.7.5. Минимални изисквания към параметрите на качеството

Системата трябва да работи в режим 7/24/365. Конкретните параметри, свързани с достигането на необходимото ниво на работоспособност през гаранционния период, са дадени в Таблицы от 1 до 5.

Таблица 1

Наличност на Системата в проценти и часове на годишна база				
Система	В рамките на работните часове	Максимално сумарно отпадане на Системата в работно време за една година	Извън рамките на работните часове	Максимално сумарно отпадане на Системата в извън работно време за една година
	99,50%	<15 часа	98,00%	<116 часа

Таблица 2

Планиране на прекъсвания (планирана недостъпност) на Системата		
Продължителност на планирана недостъпност		
< 1 час	от 1 до 6 часа	от 6 до 11 часа
По всяко време	Извън работните часове	В почивни дни или по време на официални празници
Забележка: (а) Ако планираното прекъсване може да надхвърли 11 часа, трябва да се раздели на две (или повече прекъсвания), които не превишават 11 часа. (б) Работните часове са съгласно Таблица „Дефиниции“. (с) Цитираните в таблицата данни и системи са актуални към датата на изготвяне на настоящия документ. При настъпили промени системите ще бъдат актуализирани.		

Важно: Обявяването на планирано прекъсване става посредством уведомяване на Възложителя минимум 7 работни дни предварително. Уведомяването трябва да съдържа:

- засегната/и система/и;
- начална дата и час;
- крайна дата и час;
- причина.

Таблица 3

Приоритети	
Приоритет	Въздействие върху работните процеси
1 Критичен	<u>Критично влияние</u> върху работните процеси. Изисква незабавно действие, като работата продължава до неговото отстраняване. • Пълно прекъсване на една или повече ЕАУ, предоставяни от администрацията, прекъсване работата на регистри, приложни програмни интерфейси; • Недостъпност до предоставяни през функционалността на Системата ЕАУ, които пряко и съществено засягат ключови или голям брой клиенти; • Висок риск от финансови загуби и/или засягане на имиджа на администрацията или негови контрагенти; • Създава висок риск за компрометиране на информация в Системата; • Нарушена комуникация в инфраструктурата на държавната администрация и с други държави - членки на ЕС, или на аналогични системи; • Риск за съществено прекъсване или излизане от строя на Системата; • Критична функционалност не функционира нормално или има критично и негативно отражение върху операциите на потребителите или системната среда във ведомство на Възложителя, или в имиджа на същото, или е възникнало непланирано преустановяване на достъпността.
2 Висок	<u>Съществено влияние</u> върху работните процеси. Изисква ангажиране на необходимите ресурси за отстраняването на проблема, като работата продължава в нормалните работни часове до неговото отстраняване. • Влошаване на качеството на предлагана услуга или достъп до такава, без пълно прекъсване; • Създаване на сериозен риск от възникване на инцидент с критичен приоритет; • Критична функционалност функционира непълноценно или има силно неблагоприятно отражение върху работните процеси вследствие на неприемлива производителност или генериране на грешни данни.
3 Среден	<u>Несъществено влияние</u> върху работните процеси. Изисква ангажиране на необходимите ресурси за отстраняване на проблема, като работата за неговото отстраняване е не повече от 7 работни дни. • Ограничено въздействие върху работата на Системата, което засяга или създава неудобство за изпълнение на отделни функции, без да има цялостно отражение върху функциите ѝ. Забавяне на отстраняването му може да доведе до възникване на инцидент от по-високо ниво. • Нормалната производителност на Системата или част от него е влошена, но по-голяма част от функционалната му способност е незасегната.

4 Нисък	Няма пряко влияние върху работните процеси в момента на възникването му. Изисква ангажирането на необходимите ресурси за отстраняване на проблема, като работата за неговото отстраняване е не-повече от 14 работни дни - В момента липсва пряко влияние върху функционирането на Системата, но нерешаването му в определен срок крие потенциален риск от възникване на инцидент с по-висок приоритет. - Обикновено се свързва с подобряване на функционирането на услуга, предоставяна от Системата или развитието ѝ. - Отстраняването се планира съвместно с Възложителя и е обект на средносрочно планиране. Възложителят може да изисква информация или помощ по възможните решения.
---------	---

Таблица 4

Параметри на качеството при отстраняване на инцидент				
Приоритет на инцидента	Време за реакция, max	План за решение, max	Начин на отстраняване	Срок за отстраняване на инцидента, max
1	30 минути	2 часа	В специална версия	6 часа
2	1 час	4 часа	В специална версия	12 часа
3	1 работен ден	1 седмица	В следваща версия	7 работни дни
4	1 работен ден	1 седмица	В следваща версия	14 работни дни

Забележки:

- Приоритетите се определят от Възложителя съгласно точка „Определяне на степента на критичност на инцидент“;
- За инциденти от 1 и 2 приоритет, ако за времето на отстраняване на проблема бъде намерено временно решение, с което изцяло се възстановява работоспособността на Системата, Възложителят може да понижи приоритета на инцидента, без да го закрива.
- Всички времена, посочени в таблицата, започват да текат от момента на регистриране в Системата за управление на инциденти на Възложителя.
- При обективна невъзможност да бъдат спазени сроковете в таблицата, Възложителят може да ги промени за конкретен инцидент;

Таблица 5

Параметри на качеството при отстраняване на проблем				
Приоритет на проблема	Време за реакция, max	План за решение, max	Начин на отстраняване	Срок за отстраняване на проблема, max
1	1 час	4 часа	В специална версия	24 часа
2	2 часа	24 часа	В специална версия	72 часа
3	1 работен ден	1 седмица	В следваща версия	7 работни дни

4	1 работен ден	1 седмица	В следваща версия	14 работни дни
---	---------------	-----------	-------------------	----------------

Забележки:

- За инциденти от 1 и 2 приоритет, ако за времето на отстраняване на проблема бъде намерено временно решение, с което изцяло се възстановява работоспособността на Системата, Възложителят може да понижи приоритета на инцидента, без да го закрива.
- Всички времена, посочени в таблицата, започват да текат от момента на регистриране в Системата за управление на инциденти на Възложителя.

6.7.6. Управлението на промените (Change management)

В техническото си предложение участниците трябва да предложат метод за управление на промените, който ще прилагат при изпълнението на поръчката, съобразявайки се с описаните по-долу изисквания.

Управлението на промените цели да гарантира осигуряването на:

- ускорено и устойчиво развитие в условия на намален риск на работа на Системата;
- минимизиране на неблагоприятното въздействие върху потребителите при нормалната експлоатация на електронните услуги;
- навременното внедряване само на одобрени промени и с минимални грешки;
- ефект от промяната върху всички засегнати компоненти на Системата;
- всички спешни (критични) промени да са прегледани и одобрени;
- навременно и коректно информиране на ключовите заинтересовани лица относно всички аспекти на промяната.

Процесът включва:

- Дефиниране на необходимостта и обхвата на промяната;
- Съгласуване на необходимостта и обхвата на промяната със заинтересованите страни;
- Оценка на въздействието върху бизнес процеси, системна инфраструктура или приложен софтуер, необходимия финансов ресурс, ползите и рисковете свързани с промяната;
- Подаване и регистриране на искане за промяна в Системата за управление на промените на Възложителя;
- Приоритизиране на подадени искания за промяна на база изготвена обосновка относно функционалните и техническите изисквания, необходимите ресурси, законовите и/или договорни изисквания, които налагат промяната;
- Мотивирано одобрение или отказ за одобрение на промяната;
- Планиране, управление и координиране на разработката на промяната. Изготвяне на план за разработка на промяната. В плана, ако е приложимо, се включват и дейности по конвертиране и/или миграция на данни, промени в други компоненти на Системата, засегнати услуги или инфраструктура, обслужваща Системата, промени в архивиращи процедури и/или други промени, гарантиращи успешната реализация на промяната;

- Дефиниране, управление и координиране на спешните промени с цел минимизиране на вероятността за последващи инциденти, изработване на оценка на въздействието и одобряване след внедряването на спешната промяна. Създаване на процедура за предоставяне и прекратяване на необходимия достъп до системите и информационните активи за пускане в експлоатация на спешни промени;
- Документиране, контрол и отчитане на дейностите по изпълнение на промяната (включително документиране на отхвърлените промени, проследяване на статуса на одобрените промени и приключване на процеса на промяна) с цел гарантиране, че одобрените промени са внедрени съгласно плана за внедряване на промяната;
- Актуализиране на системната документация и документацията на засегнатите работни процеси и процедури;
- Приемане на промяната и въвеждане в реална експлоатация, включва:
 - Изготвяне на план за въвеждане в експлоатация на промяната. Като в плана се включват при необходимост и дейности, които са извън обхвата на дейностите по настоящата техническа спецификация, но са предусловие за успешното реализиране на промяната. В този случай тези предусловия се ескалират до Възложителя за предприемане на действия по компетентност;
 - Дефиниране на тестови сценарии и критерии за приемане на промяната, подготовка на тестова среда и фактическо тестване на промяната;
 - Провеждане на тестове по приемане;
 - Подготовка на експлоатационната среда чрез мигриране на всички промени от тестовата среда към експлоатационната (хардуер; мрежови ресурси; операционни системи; приложен софтуер; данни за настройка на системни параметри, номенклатури, вътрешни и/или външни интерфейси; транзакционни данни) и фактическо мигриране;
 - Подготовка на участниците (компоненти на Системата и потребители) в засегнатите от промяната работни процеси, осигуряване на канали за комуникация и обучение;
 - Компилиране на нова версия, инсталиране в реална среда и първоначално съпровождане.
- Приключване на промяната;
- Отчитане на ползите и реалните ефекти от извършената промяна.

Искането за промяна може (допуска се) да се инициира и от двете страни (Възложител и Изпълнител). Упълномощени представители на Възложителя или Изпълнителя могат да инициират искане за промяна. Исканията за промяна се регистрират в Системата за управление на промени на Възложителя.

Регистрираните искания за промени се разглеждат от компетентни органи, където промените се преглеждат и се взема решение за съответното действие по тях.

7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ

Всички информационни системи и софтуерните компоненти в администрацията, в т.ч. регистри, интернет страници, вътрешни информационни системи, потребителски интерфейси към съществуващи системи, системи за предоставяне на електронни административни услуги и за електронен документооборот, трябва да отговарят на изискванията на Закона за електронното управление, Закона за киберсигурност, Закона за достъп до обществена информация и Закона за достъп до пространствени данни и подзаконовата нормативна база към тях. Неизпълнението на тези изисквания от страна на изпълнителите по договори за разработка и/или надграждане на информационни системи/ регистри/ ЕАУ е основание за неприемане на разработеното софтуерно решение от страна на Възложителя.

7.1. Функционални изисквания към информационната система

7.1.1. Интеграция с външни информационни системи

За реализиране на основни бизнес процеси Системата трябва да поддържа интеграция в реално време с хоризонталните и централните информационни системи на електронното управление, както следва:

Интеграция с хоризонталните системи на ЕУ

Интеграцията на Системата с хоризонталните системи за електронно управление се осъществява чрез разработване и внедряване на служебен интерфейс за обмен на данни, както следва:

Код	Описание	Приложимост	Забележка*
F1	Информационна система за електронна автентикация версия 2.0	Задължително, до влизане в сила на Националната схема за електронна идентификация по ЗЕИ.	
F2	Информационна система за сигурно електронно връчване	Задължително, ако е приложимо.	
F3	Информационна система за електронно плащане	Задължително за информационни системи, чрез които се извършват плащания на такси за ЕАУ с ниво на електронизация 4, и други задължения.	
F4	Информационна система за електронни форми	Задължително, ако е приложимо.	
F5	Информационна система за е-валидация	Задължително, ако е приложимо.	

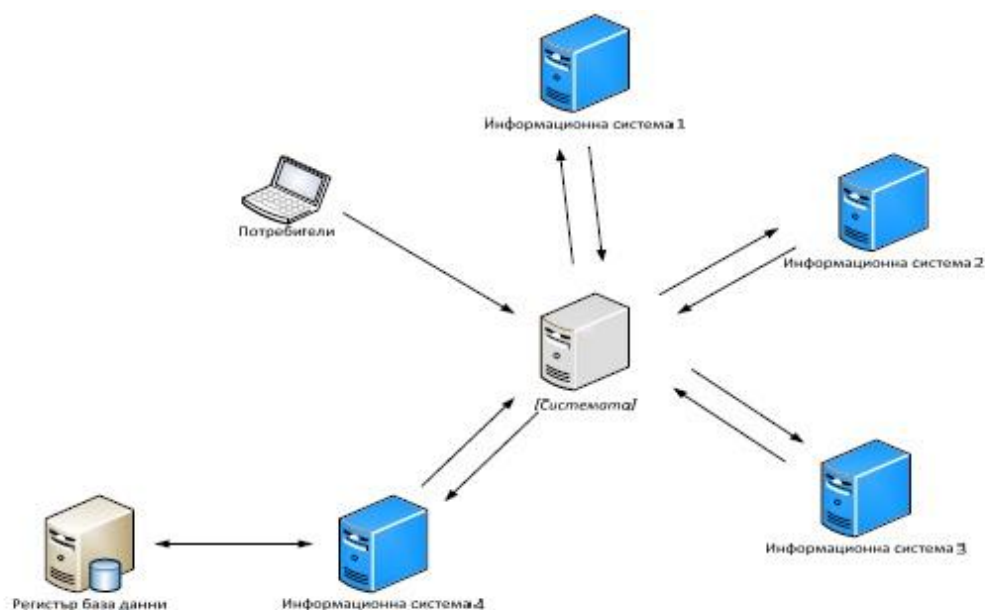
- [Информационна система 1] - [кратко описание];
- [Информационна система 2] - [кратко описание];
- [Информационна система 3] - [кратко описание].



Опишете всички информационни системи, с които е необходима интеграция, както и кратко описание за какво се използват и защо е необходима интеграция.

Изтрийте тази текстова кутия при финализиране на документа.

Код	Описание	Приложимост	Забележка*
F6	Интегрираната информационна система на държавната администрация (ИИСДА), в частност Регистъра на услугите, в който се вписват допустимите заявители и получатели на административни услуги - например: проверка на достъпа до съответните обстоятелства, посочване на идентификатор на конкретна административна услуга, за която е нужно извличането на съответните обстоятелства от регистрите;	Задължително, ако чрез Системата се предлагат ЕАУ.	
F7	При реализиране на системи за документооборота на административните органи, касаеща обмяна на електронни документи, интеграцията да се извършва съгласно технически протокол, който позволява ○ обмен на документи между различни системи за документооборота в различни администрации; ○ проследяване на движението на документа и етапа на процедурата по разглеждането или съставянето му.	Задължително, ако е приложимо.	
F8	Интеграциите с външни информационни системи и регистри трябва да се реализира чрез стандартен интеграционен слой, съгласно действащите изисквания за оперативна съвместимост	Задължително	



7.1.2. Използване на интеграционния слой на електронното управление

Интеграция на Системата чрез използване на интеграционния слой на ЕУ, включващ:

Код	Описание	Приложимост	Забележка*
F9	Интеграционна шина за обмен на справочна и удостоверителна информация (RegiX): - В случай че Системата се явява първичен регистър на данни, с цел присъединяване към интеграционната шина и впоследствие използването на първичните данни от други АО, е необходимо да се предвиди разработката на адаптер, който да се реализира съгласно стандарта, публикуван на Портала за електронно управление, в раздел „Разработчици“; - При условие че Системата използва данни от ПАД, трябва да бъде предвидена интеграция с първични регистри чрез стандартен междинен слой или чрез националната схема за електронна идентификация – конкретната реализация трябва да бъде одобрена от Възложителя след приключване на етапа на бизнес-анализ.	Задължително	
F10	Интеграционна шина за обмен на електронни документи	Задължително, когато се обменят електронни документи чрез документооборотни системи.	
F11	Интеграционна шина за достъп и управление на ИТ услуги и данни на МЕУ	Препоръчително	

F12	Информационна система за централизирано поддържане на регистри	Задължително, когато се изграждат регистри, които са били водени на хартия и не са включени в графика за привеждане на регистрите на АО в съответствие със ЗЕУ чрез ИСЦИПР (ПМС № 232/20.11.2023 г)	
F13	Да се реализира служебен интерфейс за автоматизиран онлайн обмен на данни и предоставяне на вътрешни електронни административни услуги.	Задължително	
F14	Трябва да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано машинно поискване и предаване на история на изпълнените транзакции по машинен обмен на данни, предоставените електронни услуги и начислени такси, към информационни системи на други публични институции и доставчици на обществени услуги, с оглед предоставяне на КАО, съгласно действащите изисквания за оперативна съвместимост.	Задължително, ако е приложимо.	

7.1.3. Технически изисквания към интерфейсите

Код	Описание	Приложимост	Забележка*
F15	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.	Задължително	
F16	Необходимо е да бъде разработен и внедрен служебен онлайн интерфейс за автоматизирано изпращане на транзакционна история към системата за електронна идентификация, съгласно действащите изисквания за оперативна съвместимост.	Задължително	
F17	Трябва да бъде разработен и внедрен служебен онлайн интерфейс за електронни разплащания чрез интеграция с Централен виртуален ПОС терминал, позволяващ заплащане на такси за ЕАУ и други по електронен път без дължими преводни такси и комисиони.	Задължително за информационни системи, чрез които се извършват плащания на такси за ЕАУ с ниво на електронизация 4, и други задължения	

F18	Всички публични и служебни онлайн интерфейси трябва да бъдат реализирани с поддръжка на режими "push" и "pull", в асинхронен и синхронен вариант – практическото прилагане на всяка от комбинациите трябва да бъде определено на етап бизнес анализ и да бъдат съобразени реалните казуси (use cases), които всеки интерфейс обслужва.	Ако е приложимо	
F19	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.	Задължително	
F20	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.	Задължително	

7.1.4. Електронна идентификация на потребителите

Код	Описание	Приложимост	Забележка*
F21	Електронната идентификация на всички потребители трябва да бъде реализирана в съответствие с изискванията на Регламент ЕС 910/2014 и ЗЕИ.	Задължително	
F22	влизане в сила на националната схема за електронна идентификация по ЗЕИ в Системата трябва да бъде осъществена интеграция с хоризонталната система на електронното управление – е-автентикация v2.0, която поддържа интеграция с външни доставчици на идентичност, съгласно § 5 от Преходните и заключителните разпоредби на НОИИСРЕАУ. Реализацията на интеграцията трябва да бъде осъществена по стандартни протоколи SAML 2.0 и/или OpenID Connect.	Задължително	
F23	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.	Препоръчително	
Процес по регистрация на потребители			
F24	Да се предостави възможност за визуализиране на информацията относно стъпките по регистрация и информация във връзка с процеса за потвърждаване на регистрацията и активиране на потребителския	Задължително	

	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“.		
F25	Да има възможност за избор на потребителско име с контекстна валидация на полетата (in-line validation), включително и за избраното потребителско име, и визуализиране на сложността на паролата като „слаба“, „нормална“ и „силна“.	Препоръчително	
F26	Да се реализира функционалност за потвърждение и активиране на регистрацията чрез изпращане на съобщение до регистрирания имейл адрес на потребителя, 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.	Задължително	
F27	При реализиране на вход в Системата с удостоверение за електронна идентичност, по Националната схема за електронна идентификация по ЗЕИ, Системата трябва да използва потребителския профил, създаден в нея, 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.	Задължително	
F28	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.	Задължително	

7.1.5. Отворени данни

Код	Описание	Приложимост	Забележка*
F29	Трябва да бъде разработен и внедрен автоматизиран интерфейс за осигуряване на свободен публичен автоматизиран достъп до документите, информацията и данните в Системата (наричани заедно „данните“).	Задължително за системи, които предоставят данни по ЗДОИ	

	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 обществен сектор и на Закона за достъп до обществена информация.		
F30	Трябва да бъде разработен и внедрен онлайн интерфейс за предоставяне на пространствени данни, в машинночетим, отворен формат и интеграция с Националния портал за достъп до пространствени данни съгласно всички изисквания на Директива 2007/2/ЕО и Закона за достъп до пространствени данни. Трябва да се поддържат всички набори от данни, които са изискуеми по Директива 2007/2/ЕО и за които Възложителят се явява първичен администратор на данните.	Задължително за ИС, които обработват пространствени данни	
F31	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 https://data.egov.bg/ , който съдържа връзки и метаданни за списъците с материали, съгласно изискванията на Закона за достъп до обществена информация (ЗДОИ).	Задължително за системи, които предоставят данни по ЗДОИ	
F32	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.	Задължително	
F33	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.	Задължително	

7.1.6. Формиране на изгледи

Код	Описание	Приложимост	Забележка*
F34	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; ▪ Експорт на данни в един или в няколко от изброените формати – ODF, Excel, PDF, HTML, TXT, XML, CSV и запис върху електронен носител.	Задължително	

7.1.7. Администриране на Системата

Код	Описание	Приложимост	Забележка*
F35	Системата трябва да осигурява администриране на потребителите и правата за достъп чрез административен панел, с който администраторите на системата да създават профили, управляват, назначават, отнемат роли и права на потребителите.	Задължително	

7.2. Нефункционални изисквания към информационната система

7.2.1. Авторски права и изходен код

Код	Описание	Приложимост	Забележка*
NF1	Всички компютърни програми, които се разработват за реализиране на Системата, трябва да отговарят на критериите и изискванията за софтуер с отворен код.	Задължително	
NF2	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.	Задължително	
NF3	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; • Mozilla Public License 2.0 • EUPL (European Union Public License).	Задължително	
NF4	Изходният код (Source Code), разработван по проекта, както и цялата техническа документация трябва да 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 глава шеста, раздел IV „Хранилище за изходен код“ от НОИИСРЕАУ.	Задължително	
NF5	Избраният подход за изграждане на резултатния продукт (Системата) трябва да бъде детайлно описан в техническото предложение на участниците. Да се изследва възможността резултатният продукт	Задължително	

	(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.		
NF6	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.	Задължително	

7.2.2. Системна и приложна архитектура

Код	Описание	Приложимост	Забележка*
NF7	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. 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.	Задължително	
NF8	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.	Препоръчително	
NF9	При разработката, тестването и внедряването на Системата Изпълнителят трябва да прилага наложими 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).	Задължително	

NF10	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.	Задължително	
NF11	Приложните програмни интерфейси и информационните обекти задължително да поддържат атрибут за версия.	Задължително	
NF12	Програмните интерфейси, изискуемите метаданни и атрибути за версия и достъп до стари версии трябва задължително да са налични и готови за използване минимум 24 месеца след публикуване на нова версия.	Задължително	
NF13	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).	Задължително	
NF14	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).	Задължително	
NF15	Системата трябва да осигурява възможности за разширяване, резервиране и балансиране на натоварването между множество инстанции на сървъри с еднаква роля.	Задължително	
NF16	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.	Задължително	
NF17	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,	Задължително	

	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.		
NF18	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).	Задължително	
NF19	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 прониквания чрез прилагане на подходящи политики за мрежова и информационна сигурност от Възложителя в инфраструктурата на Държавния хибриден частен облак и ЕЕСМ.	Задължително	
NF20	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.	Задължително	
NF21	Системата трябва да бъде разработена така, че да позволява използването ѝ от много различни институции (т.нар. multitenancy), като за използване от нова институция не трябва да се изисква нова инсталация.	Задължително, ако е приложимо	
NF22	Трябва да бъде създаден административен интерфейс, чрез който може да бъде извършвана конфигурацията на софтуера.	Задължително	
NF23	Всеки обект в системата трябва да има уникален идентификатор.	Задължително	
NF24	Записите в регистрите не трябва да подлежат на изтриване или на промяна, а всяко изтриване или промяна трябва да представлява нов запис	Задължително	

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

Код	Описание	Приложимост	Забележка*
NF25	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.	Задължително	
NF26	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.	Задължително	
NF27	Използването на софтуер със затворен код 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.	Задължително	
NF28	Ако Изпълнителят предложи внедряване на Системата чрез използване на софтуерно решение със затворен код, то той трябва да обоснове, че това решение е икономически по-изгодно, отколкото разработка на софтуерно решение с отворен код.	Задължително	
NF29	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.	Препоръчително	

NF30	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 (https://git.egov.bg/explore/projects). Използващите свободните библиотеки компоненти задават за „upstream repo“ хранилищата, като задължително се реферира използваната версия/ commit identifier.	Задължително	
NF31	Когато се налага промяна в изходния код на използван софтуерен компонент, промените трябва да се извършват във fork хранилището 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.	Задължително	

7.2.4. Изграждане и поддръжка на множество среди

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

Среда	Описание
Среда за развойна дейност (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.
Staging	Чрез Staging средата се извършват тестове преди разгръщане на нова версия от Development средата върху Production средата. В нея се извършват всички интеграционни тестове, както и тестове за натоварване.
Тестова (Sandbox, Testing)	Чрез Sandbox средата всички, които трябва да се интегрират към Системата, могат да тестват интеграцията си, без да застрашават работата на продукционната среда.
Продукционна (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

Код	Описание	Приложимост	Забележка*
NF32	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 те биха могли да съдействат в процесите по развитие и тестване на разработките през целия им жизнен цикъл.	Задължително	
NF33	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 (https://git.egov.bg/explore/projects). 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.	Задължително.	
NF34	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 <i>(в случай на надграждане на съществуваща система – 50% от новата функционалност и 20% от съществуващата)</i>; - Използване на continuous integration практики; - Използване на dependency management. Участникът трябва да опише детайлно подхода си за покриване на изискванията.	Задължително	

NF35	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.	Задължително	
-------------	---	--------------	--

7.2.6. Бързодействие и мащабируемост

7.2.6.1. Контрол на натоварването и защита от DoS/ DDoS атаки

Код	Описание	Приложимост	Забележка*
NF36	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.	Задължително	
NF37	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.	Задължително	
NF38	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.	Задължително	

7.2.6.2. Кохерентно кеширане на данни и заявки

Код	Описание	Приложимост	Забележка
NF39	Отделните информационни системи, подсистеми и интерфейси трябва да бъдат проектирани и да използват системи за разпределен кохерентен кеш в случаите, в които това би довело до подобряване на производителността и мащабируемостта, чрез спестяване на заявки към СУБД или файловите системи на сървърите.	Задължително	
NF40	Изпълнителят трябва да опише детайлно подхода и използваните механизми и технологии за реализация на разпределения кохерентен кеш, както и системните компоненти, които ще използват разпределения кеш.	Задължително	
NF41	Разпределеният кохерентен кеш трябва да поддържа възможност за компресия на подходящите за това данни – например тези от текстов тип; компресирането на данни може да бъде реализирано и на приложно ниво.	Задължително	

NF42	Използваният алгоритъм за създаване на ключове за съхранение/намиране на данни в кеша не трябва да допуска колизии и трябва оптимално да използва процесорните ресурси за генериране на хешове.	Задължително	
NF43	Изпълнителят трябва да подбере подходящи софтуерни решения с отворен код за реализиране на буфериране и кеширане на данните в оперативната памет на сървърите. В зависимост от конкретните приложни случаи (Use Cases) е допустимо да се използват и внедрят различни технологии, които покриват по-добре конкретните нужди – например решения като Memcached или Redis в комбинация с Redis GeoAPI могат да осигурят порядъци по-висока мащабируемост и производителност за често достъпвани оперативни данни, номенклатурни данни или документи.	Задължително	
NF44	Като минимум разпределен кохерентен кеш трябва да се предвиди при: ▪ Извличане на информация от номенклатури и атомични данни за статус и актуално състояние на партии от регистри в информационните системи; ▪ Извличане на информация от предефинирани периодични справки; ▪ Информация от лога на транзакциите при достъп с електронно-ИД до дадена услуга; ▪ Информация за извършените плащания; ▪ Други, които са идентифицирани на етап бизнес и системен анализ. От кеша следва да бъдат изключени прикачени файлове и големи по обем резултати от справки.	Задължително	

7.2.6.3. Бързодействие

Код	Описание	Приложимост	Забележка*
NF45	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 <i>[В случай че функционалните изисквания предвиждат визуализация на справки или сложни електронни документи, изискването се адаптира, като се съобразява спецификата на функционалността]</i> . Трябва да бъдат създадени тестове за натоварване.	Задължително	

7.2.6.4. Използване на HTTP/2

Код	Описание	Приложимост	Забележка*
NF46	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.).	Задължително	
NF47	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).	Задължително	
NF48	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.	Задължително	

7.2.6.5. Подписване на документи

Код	Описание	Приложимост	Забележка*
NF49	При реализацията на електронно подписване с всички видове електронен подпис трябва да се подписва сигурен хеш-ключ, генериран на базата на образа/съдържанието, а не да се подписва цялото съдържание.	Задължително	
NF50	Минимално допустимият алгоритъм за хеширане, който трябва да се използва при електронно подписване, е SHA-256. В случаите, в които не се подписва уеб съдържание (например документи, файлове и др.), е необходимо да се реализира поточно хеширане, като се избягва зареждането на цялото съдържание в оперативната памет.	Задължително	
NF51	Системата трябва да поддържа подписване на електронни изявления и електронни документи и с електронни подписи, издадени от Доставчици на доверителни услуги в ЕС, които отговарят на изискванията за унифициран профил на електронните подписи, съгласно подзаконовите правила към Регламент ЕС 910/2014, които влизат в сила и са задължителни от 1 януари 2017 г.	Задължително	

NF52	Трябва да бъдат анализирани техническите възможности за реализиране на подписване на електронни изявления и документи без използване на Java аplet и без да се изисква от потребителите да инсталират Java Runtime, като по този начин се осигури максимална съвместимост на процеса на подписване с всички съвременни браузъри. Такава реализация може да бъде осъществена чрез: ■ използване на стандартни компоненти с отворен код, отговарящи на горните условия, които са разработени по други проекти на държавната администрация и са достъпни в хранилището, поддържано от Министерство на електронното управление – при наличие на такива компоненти в хранилището те трябва да се преизползват и само да бъдат интегрирани в Системата; ■ използване на плагин-модули с отворен код, достъпни за най-разпространените браузъри (Browser Plug-ins), които са адаптирани и поддържат унифицираните профили на електронните подписи, издавани от доставчик на удостоверителни услуги в ЕС, и съответните драйвери за крайни устройства за четене на сигурни носители или по стандартизиран в националната нормативна уредба протокол за подписване извън браузъра; ■ чрез интеграция с услуги за отдалечено подписване, предлагани от доставчици на доверителни услуги в ЕС.	Задължително	
-------------	--	--------------	--

7.2.6.6. Качество и сигурност на програмните продукти и приложенията

Код	Описание	Приложимост	Забележка*
NF53	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);	Задължително	
NF54	Публичните модули, които ще предоставят информация и електронни услуги в Интернет, трябва да отговарят на актуалните web стандарти за визуализиране на съдържание.	Задължително	

7.2.7. Информационна сигурност и интегритет на данните

Код	Описание	Приложимост	Забележка*
NF55	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	Задължително	

	пароли и където е възможно, да се използва и прозрачно криптиране на данните в СУБД със сертификати (transparent data-at-rest encryption).		
NF56	Да бъде предвидена система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата.	Задължително	
NF57	Не се допуска използването на Self-Signed сертификати за публични услуги.	Задължително	
NF58	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 удостоверяващ орган, разпознаван от най-често използваните браузъри (Microsoft Internet Explorer, Google Chrome, Mozilla Firefox). Ежегодното преиздаване и подновяване на сертификата трябва да бъде включено като разходи и дейности в гаранционната поддръжка за целия срок на поддръжката.	Задължително	
NF59	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-а. Схемата за проксиране на заявките трябва да бъде защитена от Spoofing.	Задължително	
NF60	Като временна мярка за съвместимост настройките на web сървърите 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.	Задължително	
NF61	При разгръщането на всички web услуги (Web Services) трябва да се използва единствено протокол HTTPS със задължително прилагане на минимум TLS 1.2.	Задължително	
NF62	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 минималните изисквания за мрежова и информационна сигурност.	Задължително	

NF63	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).	Задължително	
NF64	Трябва да бъде изграден модул за проследимост на действия и събития в Системата. Записът 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.	Задължително	
NF65	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.	Задължително	
NF66	Астрономическото време за удостоверяване настъпването на факти с правно значение и на такива, за които се изисква противопоставеност, 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 от доставчик на доверителни услуги или от държавен орган, осигуряващ такава услуга, отговаряща на изискванията на RFC 3161.	Задължително	
NF67	Трябва да бъдат проведени тестове за проникване (penetration tests), с които да се идентифицират и коригират слаби места в сигурността на Системата.	Задължително	
NF68	При идентификация на регистри и бази данни да се използва електронно удостоверение във формат X.509, издаден за съответния регистър. Идентификацията се осъществява двустранно по протокол TLS (Transport Layer Security - Сигурност на транспортния слой), версия 1.2 или по-висока, дефиниран в Препоръка RFC 5246, приета от IETF.	Задължително	
NF69	Информационните системи на административните органи да се идентифицират пред регистрите чрез цифров сертификат, двустранно по протокол TLS (Transport Layer Security - Сигурност на транспортния слой), версия 1.2 или по-висока.	Задължително	

7.2.8. Използваемост

7.2.8.1. Общи изисквания за използваемост и достъпност

Код	Описание	Приложимост	
NF70	При проектирането и разработката на интернет страници и мобилни приложения трябва да се спазват стандартите за достъпност на потребителския интерфейс за хора с увреждания WCAG 2.1.	Задължително	
NF71	Съдържанието на интернет страниците и мобилните приложения на административните органи, на доставчиците на обществени услуги и на лицата, осъществяващи публични функции, трябва да отговаря на последната обнародвана в „Официалния вестник“ на Европейския съюз версия на хармонизирания стандарт EN 301 549, освен в случаите по чл. 58в, ал. 2 или 3 от ЗЕУ.	Задължително	
NF72	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 на заявление, за генериране на справка и други.	Задължително	
NF73	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). При използване на Captcha се осигуряват алтернативни форми с използване на изходи за различни видове сетивни възприятия, съобразени с различните увреждания.	Задължително	
NF74	Не се допуска използване на 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 идентифицирани много последователни опити от предполагаем „бот“.	Задължително	
NF75	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.	Задължително	

NF76	Публичните уебстраници на Системата трябва да бъдат проектирани и оптимизирани за ефективно и бързо индексирание 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 автоматизирани 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.	Задължително	
NF77	Не се допуска използването на HTML Frames, за да не се пречи на оптимизациите за търсещи машини.	Задължително	
NF78	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/json-ld/); ○ Open Graph Protocol (http://ogp.me) за осигуряване на поддръжка за качествено споделяне на ресурси в социални мрежи и мобилни приложения.	Задължително	
NF79	В екранните форми на Системата трябва да се използват потребителски бутони с унифициран размер и лесни за разбиране текстове в еднакъв стил.	Задължително	
NF80	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).	Задължително	
NF81	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.	Задължително	
NF82	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.	Задължително	
NF83	Всички търсения трябва да са нечувствителни към малки и главни букви.	Задължително	
NF84	Полетата за пароли трябва задължително да различават малки и главни букви.	Задължително	

NF85	Полетата за потребителски имена трябва да позволяват използване на имейл адреси като потребителско име, включително да допускат всички символи, регламентирани в RFC 1123, за наименоуването на хостове.	Задължително	
NF86	Главните и малките букви на въвежданите данни се запазват непроменени, не се допуска Системата да променя капитализацията на данните, въвеждани от потребителите.	Задължително	
NF87	Системата трябва да позволява въвеждане на данни, съдържащи както български, така и символи на официалните езици на ЕС.	Задължително	
NF88	Наименованията на полетата следва да са достатъчно описателни, като максимално се доближават до характера на съдържащите се в тях данни.	Задължително	
NF89	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.	Задължително	
NF90	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.	Задължително	
NF91	За големите йерархически категоризации трябва да се предвиди възможност и за навигация по нива или чрез отложено зареждане (lazy load).	Задължително	
NF92	Интернет страниците на администрациите трябва отговарят на правилата за институционална идентичност, определени от министъра на електронното управление. Наименованията на домейните и поддомейните, използвани от административните органи за официалните им интернет страници и портали, трябва да отговарят на изискванията на чл. 47 от НОИИСПЕАУ. Ако се използват споделени информационни ресурси от ДХЧО за инсталиране на Системата, за публичен достъп в интернет може да се използват поддомейни на egov.bg със следната конвенция: [име на система].egov.bg. Например: iara-iss.egov.bg, strategy.egov.bg и др.	Задължително	

7.2.8.2. Интернационализация

Код	Описание	Приложимост	Забележка
NF93	Системата трябва да може да съхранява и едновременно да визуализира данни и съдържание, което е въведено/генерирано на различни езици.	Задължително	
NF94	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, web услугите 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.	Задължително	
NF95	Всички публично достъпни потребителски интерфейси следва да поддържат многоезичност, като минимум български и английски език.	Задължително	
NF96	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.	Задължително	
NF97	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 таксономииите и др. Данните, които се съхраняват в Системата само на български език, се изписват/визуализират на български език.	Задължително	
NF98	Системата трябва да позволява превод на всички многоезични текстове с подходящ потребителски интерфейс, достъпен за администратори на Системата, без промени в изходния код. Модулът за превод на текстове, използвани в Системата, трябва да поддържа и контекстни референции, които да позволяват на администраторите да тестват и да проверяват бързо и лесно направените преводи и тяхната съгласуваност в реалните екрани, страници и документи.	Задължително	

NF99	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.	Задължително	
NF100	При визуализация на числа трябва да се използва разделител за хиляди (интервал).	Задължително	
NF101	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 избория 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.	Задължително	

7.2.8.3. Изисквания за използваемост на потребителския интерфейс

Код	Описание	Приложимост	Забележка
NF102	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; - 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.	Задължително	
NF103	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.	Задължително	

NF104	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.	Задължително	
NF105	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.	Задължително	
NF106	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.	Задължително	
NF107	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.	Задължително	
NF108	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.	Задължително	
NF109	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.	Задължително	
NF110	Потребителският интерфейс следва да бъде достъпен за хора с увреждания съгласно изискванията на чл. 48, ал. 5 от ЗОП.	Задължително	

7.2.8.4. Изисквания за използваемост в случаи на прекъснати бизнес процеси

Код	Описание	Приложимост	Забележка
NF111	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.	Задължително	
NF112	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.	Задължително	
NF113	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 типа 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.	Задължително	

7.2.8.5. Изисквания за проактивно информиране на потребителите

Код	Описание	Приложимост	Забележка
NF114	За всички публични интернет страници трябва да бъде реализирана функционалност за публикуване на всяко периодично обновявано съдържание (новини, обявления, обществени поръчки, отворени работни позиции, нормативни документи, отговори по ЗДОИ и др.) в стандартен формат (RSS 2.x, Atom или еквивалент), както и поддържането на публично достъпни статистики за посещаемостта на страницата.	Задължително	

NF115	Системата трябва да поддържа възможност за автоматично генериране на електронни бюлетини, които да се разпращат периодично или при настъпване на събития по електронна поща до регистрираните в Системата потребители, които са заявили или са се съгласили да получават такива бюлетини; Потребителите трябва да имат възможност да настройват предпочитанията през потребителския си профил в Системата.	Задължително	
--------------	--	--------------	--

7.2.9. Системен журнал

Код	Описание	Приложимост	Забележка
NF116	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.	Задължително	
NF117	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.	Задължително	
NF118	Специална фоновая 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.	Задължително	
NF119	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.	Задължително	
NF120	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.	Задължително	

7.2.10. Дизайн на бази данни и взаимодействие с тях

Код	Описание	Приложимост	Забележка
NF121	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.	Задължително	
NF122	Базата данни трябва да може да оперира в клъстер, в определени случаи следва да бъде използван т.нар. sharding.	Задължително	
NF123	Имената на таблици и колоните трябва да следват унифицирана конвенция.	Задължително	
NF124	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.	Задължително	
NF125	Връзките между таблици трябва да са дефинирани чрез foreign key.	Задължително	
NF126	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	
NF127	Задължително трябва да се използват транзакции, като нивото на изолация трябва да бъде мотивирано в предадената документация.	Задължително	
NF128	При операции върху много записи (batch) следва да се избягват дългопродължаващи транзакции.	Задължително	
NF129	Заявките трябва да бъдат ограничени в броя записи, които връщат.	Задължително	
NF130	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).	Задължително	
NF131	При използване на нерелациона база данни трябва да се използват по-бързи и компактни протоколи за комуникация, ако такива са достъпни.	Задължително	
NF132	При обработката на данните да се спазват формализираните описания, които подлежат на задължително унифициране: 1. имена; 2. адрес; 3. единен граждански номер; 4. личен номер на чужденец; 5. ЛН - личен номер (за гражданите на Европейския съюз и техните семейства); 6. единен идентификационен код, определен от	Задължително	

	Агенцията по вписванията; 7. единен идентификационен код (код по БУЛСТАТ); 8. служебен номер по чл. 84, ал. 3 от Данъчно-осигурителния процесуален кодекс; 9. наименование на юридическо лице; 10. телефонни номера; 11. други, определени от министъра на електронното управление.		
NF133	Във връзка с изискванията за оперативна съвместимост, при разработка на Системата да се предвиди: • използването на дефинираните вече обекти в Регистъра на информационните обекти; • вписване на формализирани описания на данните, ако чрез Системата се обработват данни, за които АО е първичен администратор.	Задължително	

7.2.11. Изисквания по отношение на киберсигурност в съответствие с чл. 12, ал. 1 от НМИМС

С цел достигане на изискваното ниво на сигурност на информацията, в мрежите и информационните системи следва да се предвидят следните изисквания:

Код	Описание	Приложимост	Забележка
NF134	Да бъдат включени адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване.	Задължително	
NF135	Да се представят анализ и оценка на риска, които да послужат като основа за включването на адекватни и комплексни изисквания за мрежова и информационна сигурност.	Задължително	
NF136	Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.	Задължително	
NF137	Да се използва отделна, изолирана от другите информационни и комуникационни системи и от интернет, подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти. Тази среда трябва да не се използва за други цели.	Задължително	

NF138	Да се валидират всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя, и съдържанието на брауъра, като headers на препращащия и потребителски агент.	Задължително	
NF139	Всички данни да бъдат кодирани с HTML, изпращани от клиента и показвани в уебстраница.	Задължително	
NF140	Да се ограничават заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL.	Задължително	
NF141	Да се конфигурират типът и размерът на headers, които уебсървърът ще приеме.	Задължително	
NF142	Да се ограничава времетраенето на връзката (connection Timeout) - времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и минималният брой байтове в секунда при изпращане на отговор на заявка.	Задължително	
NF143	Да се въведе ограничение на броя неуспешни опити за влизане в системата.	Задължително	
NF144	Да не се допуска извеждането на списък на уебдиректориите.	Задължително	
NF145	Бисквитките (cookies) задължително да имат: • флаг за защита (security flag), който инструктира брауъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали; • флаг HTTP only, който инструктира брауъра, че „бисквитката“ може да бъде достъпна само от сървър, а не от скриптовете, от страна на клиента.	Задължително	
NF146	Да се предвидят и предприемат мерки за защита на DNS, като задължително се прилага DNSSEC (Domain Name System Security Extensions);	Задължително	
NF147	По отношение на системните записи (Logs) да бъдат предвидени следните възможности: • в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;	Задължително	

- за всяко от тези събития в записите се отбелязва с астрономическото време, когато е настъпило събитието;
- да бъде предвидена възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи, като се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;
- да се предвиди как информацията ще бъде архивирана за срок, не по-кратък от дванадесет месеца.

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

8.1. Дейност 1 [Наименование на дейността]

- 8.1.1. *Описание на дейността*
- 8.1.2. *Изисквания към изпълнение на дейността*
- 8.1.3. *Очаквани резултати*

8.2. Дейност 2 [Наименование на дейността]

- 8.2.1. *Описание на дейността*
- 8.2.2. *Изисквания към изпълнение на дейността*
- 8.2.3. *Очаквани резултати*

8.3. Дейност 3 [Наименование на дейността]

- 8.3.1. *Описание на дейността*
- 8.3.2. *Изисквания към изпълнение на дейността*
- 8.3.3. *Очаквани резултати*

8.4. Дейност 4 [Наименование на дейността]

- 8.4.1. *Описание на дейността*
- 8.4.2. *Изисквания към изпълнение на дейността*
- 8.4.3. *Очаквани резултати*

8.5. Дейност 5 [Наименование на дейността]

- 8.5.1. *Описание на дейността*
- 8.5.2. *Изисквания към изпълнение на дейността*
- 8.5.3. *Очаквани резултати*

9. ДОКУМЕНТАЦИЯ

9.1. Изисквания към документацията

- Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително 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 web услуги, 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 web услуга;

- 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;
- само в електронен формат, като 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 следните 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 изпращат от Изпълнителя по договора чрез системата за сигурно електронно връчване или на официалния е-мейл на Възложителя. Докладите се одобряват от отговорния/отговорните служител/служители в срок до 5 работни дни. Възложителят задължително влиза в своята деловодна система преписката по договора.

Всички доклади трябва да се представят на възложителя на български език 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)

Приложение	№	2
към	38,	4
чл.	ал.	
(Ново – ДВ, бр. 80 от 2024 г.)		

[Възложител]
ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ
за
[Име на проект]

Приложим само за дейности по адаптиране на информационните системи, регистри или бази данни във връзка с въвеждане на еврото в Република България!

СЪДЪРЖАНИЕ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ
 - 1.1. Използвани акроними
 - 1.2. Технологични дефиниции
 - 1.3. Дефиниции за нива на електронизация на услугите
2. ВЪВЕДЕНИЕ
 - 2.1. Цел на документа
 - 2.2. За възложителя – функции и структура
 - 2.3. За проекта
 - 2.4. Нормативна рамка
3. ЦЕЛИ, ОБХВАТ И ОЧАКВАНИ РЕЗУЛТАТИ ОТ ИЗПЪЛНЕНИЕ НА ПРОЕКТА
 - 3.1. Общи и специфични цели на проекта
 - 3.2. Обхват на проекта
 - 3.3. Целеви групи
 - 3.4. Очаквани резултати
 - 3.5. Период на изпълнение
4. ТЕКУЩО СЪСТОЯНИЕ
5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА
 - 5.1. Общи изисквания към изпълнението на обществената поръчка
 - 5.2. Управление на проекта
 - 5.3. Управление на риска
6. ЕТАПИ НА ИЗПЪЛНЕНИЕ НА ПРОЕКТА
 - 6.1. Анализ на данните и изискванията
 - 6.2. Изготвяне на системен проект
 - 6.3. Разработване на софтуерното решение
 - 6.4. Тестване
 - 6.5. Внедряване
 - 6.6. Обучение
 - 6.7. Гаранционна поддръжка
7. ОБЩИ ИЗИСКВАНИЯ ЗА ИНФОРМАЦИОННИ СИСТЕМИ В ДЪРЖАВНАТА АДМИНИСТРАЦИЯ
 - 7.1. Интеграция с външни информационни системи
 - 7.2. Авторски права и изходен код
 - 7.3. Системна и приложна архитектура
 - 7.4. Качество и сигурност на програмните продукти и приложенията
 - 7.5. Информационна сигурност и интегритет на данните
 - 7.6. Системен журнал
 - 7.7. Дизайн на бази данни и взаимодействие с тях
 - 7.8. Специфични изисквания при адаптиране на ИС за работа с евро

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА
 - 8.1. Дейност 1 [Наименование на дейността]
 - 8.1.1. Описание на дейността
 - 8.1.2. Изисквания към изпълнение на дейността
 - 8.1.3. Очаквани резултати
 - 8.2. Дейност ... [Наименование на дейността]
 - 8.2.1. Описание на дейността
 - 8.2.2. Изисквания към изпълнение на дейността
 - 8.2.3. Очаквани резултати
9. ДОКУМЕНТАЦИЯ
 - 9.1. Изисквания към документацията
 - 9.2. Прозрачност и отчетност
 - 9.3. Системен проект
 - 9.4. Техническа документация
 - 9.5. Протоколи
 - 9.6. Комуникация и доклади
 - 9.6.1. Встъпителен доклад
 - 9.6.2. Междинни доклади
 - 9.6.3. Окончателен доклад
10. РЕЗУЛТАТИ

1. РЕЧНИК НА ТЕРМИНИ, ДЕФИНИЦИИ И СЪКРАЩЕНИЯ

1.1. Използвани акроними

Акроним	Описание
АИС	Автоматизирана информационна система
АМС	Администрация на Министерския съвет
АО	Административен орган
АОП	Агенция по обществени поръчки
АПК	Административнопроцесуален кодекс
БУЛСТАТ	Регистър Булстат
МЕУ	Министерство на електронното управление
ЗВЕРБ	Закон за въвеждане на еврото в Република България
ЗДОИ	Закон за достъп до обществена информация
ЗЕУ	Закон за електронното управление
ЗКИ	Закон за кредитните институции
ИС	Информационна система
ИТ	Информационни технологии
КАО	Комплексно административно обслужване
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 базата на съществуваща физическа свързаност, предоставена от МЕУ, 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.
Машинночитим 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 на 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 на услуги изцяло по електронен път, включително електронно подаване на данни и документи, електронна обработка на формуляри и електронна идентификация на потребителите, освен ако със закон се допуска предоставяне на електронна административна услуга без идентификация.
Ниво 4	Извършване на услуги от ниво 3, за които е осигурена възможност за електронно връчване и електронно плащане, ако за получаването на електронна административна услуга се дължат такси.

2. ВЪВЕДЕНИЕ

2.1. Цел на документа

Целта на настоящия документ е да опише софтуерните изисквания към изпълнението на обществена поръчка с предмет: *[опишете предмета на поръчката]* за адаптирането на *[наименование на информационната система]* във връзка с присъединяването на Република България към Евророната.

В настоящата техническа спецификация са описани и изискванията към проектната организация, документацията и отчетността.

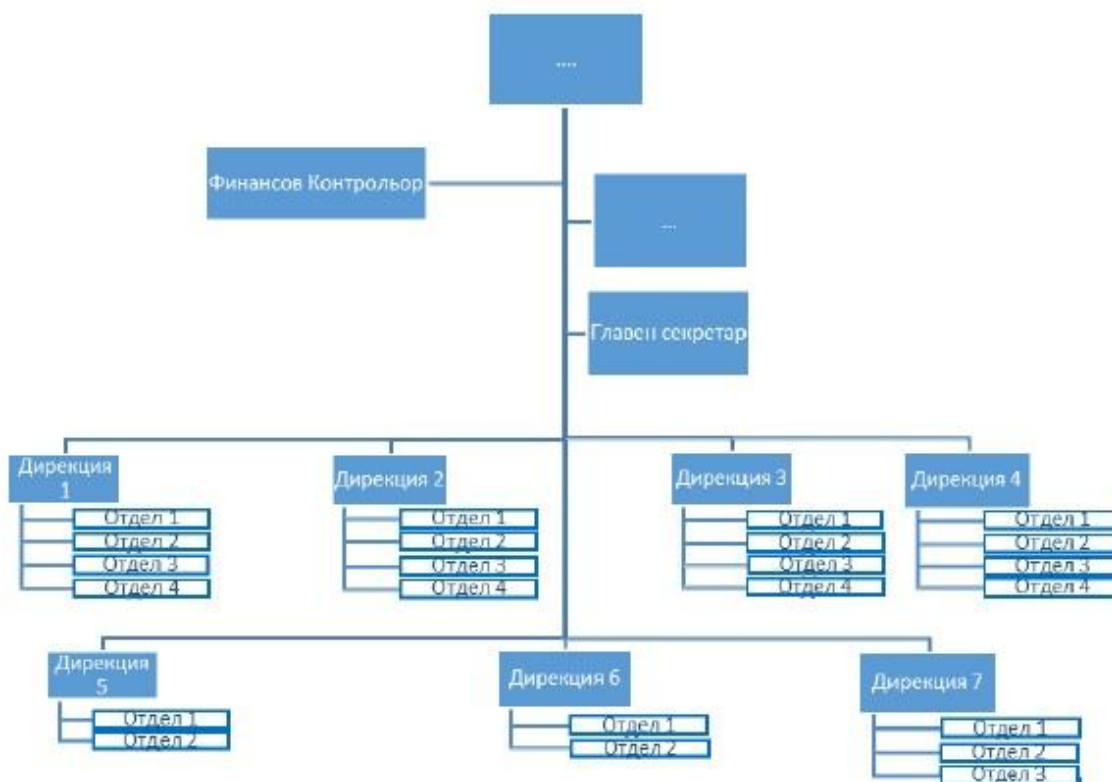
2.2. За възложителя – функции и структура



Опишете накратко функциите на Вашата администрация.

Изтрийте тази текстова кутия при финализиране на документа.

Структурата на [възложителя] е представена във Фигура 1:



Фигура 1. Структура на [възложителя]

2.3. За проекта



Кратка информация за проекта, задължително включваща:

1. Категоризация на системата съгласно Методическите указания към административните органи относно адаптирането на информационните системи във връзка с въвеждането на еврото в Република България [Настоящият образец се използва само за информационни системи категория 2, чиито авторски права са собственост на АО и за които има осигурена поддръжка, но без клауза за прилагане на нормативни промени (национално и европейско законодателство), или не е осигурена поддръжка. В този случай адаптирането за работа с евро следва да се възложи от АО с отделен договор или проект за надграждане или промяна];
2. Писмо (изходящ номер и дата), с което е удостоверено съответствието на техническа спецификация, на базата на която информационната система е разработена/надградена/внедрена, с изискванията на чл. 58а от ЗЕУ.

Изтрийте тази текстова кутия при финализиране на документа.

2.4. Нормативна рамка

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

- *Закон за електронното управление (ЗЕУ);*
- *Наредба за общите изисквания към информационните системи, регистрите и електронните административни услуги;*
- *Закон за електронния документ и електронните удостоверителни услуги;*
- *Закон за киберсигурност;*
- *Наредба за минималните изисквания за мрежова и информационна сигурност.*
- *Актуализиран Национален план за въвеждане на еврото в Република България, приет с Решение № 797 на Министерския съвет от 13 ноември 2023 г. (Националния план) и Методически указания към административните органи относно адаптирането на информационните системи във връзка с въвеждането на еврото в Република България (Методическите указания), приложение към Националния план;*
- *Закон за въвеждане на еврото в Република България (ЗВЕРБ);*
- *[Документ 1]*
- *[Документ ...]*

3. ЦЕЛИ, ОБХВАТ И ОЧАКВАНИ РЕЗУЛТАТИ ОТ ИЗПЪЛНЕНИЕ НА ПРОЕКТА

3.1. Общи и специфични цели на проекта

Проектът е насочен към адаптиране за работа с евро на *[наименование на информационната система]* във връзка с приемането на Република България в Еврозоната и при спазване на основните принципи, правила и процедури за въвеждане на еврото като парична единица на Република България, заложиени в Националния план, Методическите указания и ЗВЕРБ.

[Допълнително описание на общата цел на проекта].

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

- *[Специфична цел 1]*
- *[Специфична цел ...]*

3.2. Обхват на проекта

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

- *Дейност 1 [Наименование на дейността]*
- *Дейност ... [Наименование на дейността]*

Подробна информация за конкретните дейности по проекта е публично достъпна на адрес *[Моля, опишете].*

3.3. Целеви групи

Целевите групи, към които е насочен проектът, обхващат:

- *[Целева група 1];*
- *[Целева група ...].*

[Описват се целевите групи, посочени в Техническата спецификация на разработената и въведена в експлоатация Система, чието съответствие е удостоверено на предходен етап по реда на чл. 58б от Закона за електронното управление.]

3.4. Очаквани резултати

Надградената система *[Наименование на информационната система]* ще отговори изцяло на новите изисквания след приемане на Република България в Евронзоната.

Допълнително постигнати резултати:

- *[Резултат 1];*
- *[Резултат ...].*

3.5. Период на изпълнение

3.5.1. Периодът на изпълнение е [X] месеца, но не по-късно от [ДД.ММ.ГГГГ] г.

3.5.2. 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 със срока по т. 3.5.1.

4. ТЕКУЩО СЪСТОЯНИЕ

5. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА



Опишете текущото състояние на информационната система и бизнес процесите, които имат отношение към предмета на процедурата за адаптиране на информационната система във връзка с въвеждане на еврото в Република България.

Представете детайлна информация за системната и технологична архитектура на въведената в редовна експлоатация ИС, както и друга приложима информация, необходима за анализ и оценка на обема и вида дейности по адаптиране на Системата във връзка с въвеждане на еврото в Република България.

*Посочете линк към хранилището на МЕУ (<https://dev.egov.bg/PDev/>) с изходния код на *[наименование на информационната система]*.*

Изтрийте тази текстова кутия при финализиране на документа.

5.1. Общи изисквания към изпълнението на обществената поръчка

Обществената поръчка се изпълнява в рамките на *[Наименование на проекта/дейността]*, финансиран по *[Източник на финансиране]*. Изпълнителят следва да спазва всички нормативни изисквания по отношение на дейността на *[бенефициента]* и електронното управление в Република България.

5.2. Управление на проекта²

[Моля, изтрийте ненужното!] Участниците трябва да предложат методология за управление на проекта, която смятат да приложат, като се изтъкнат ползите ѝ за успешното изпълнение на проекта. Предложената методология трябва да съответства

² Под „проект“ следва да се разбира предметът на настоящата обществена поръчка

на най-добрите световни практики и препоръки (например Project Management Body of Knowledge (PMBOK) Guide, PRINCE2, Agile/SCRUM/Kanban, RUP и др. еквивалентни).

[Моля, изтрийте ненужното!] Възложителят изисква методология за управление на проекта, която участниците трябва да приложат и която съответства на най-добрите практики и препоръки, а именно *[Моля, опишете]*.

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;
- 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.

5.3. 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;
- Неинформирание 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

Във връзка с присъединяването на Република България към Евроразоната и адаптирането на информационни системи за работа с евро, в рамките на дейността е необходимо да се извърши цялостен анализ на текущото състояние на *[наименование на информационната система]* и да се идентифицират необходимите действия, концепции, ресурси и срокове, касаещи нейното адаптиране, съобразно заложените в Националния план, Методическите указания и ЗВЕРБ правила и принципи.

В случай че чрез информационната система се предоставят електронни административни услуги от 4-то ниво, които са свързани със заплащане на такси, е необходимо да се адаптира тарифирането им така, че да отговаря на изискванията на Националния план, Методическите указания и ЗВЕРБ, като същевременно се съхраняват всички версии на тарифите за услуги.

Анализът подлежи на одобрение от Възложителя в рамките на [X] дни от предоставянето му от Изпълнителя.

6.2. Изготвяне на системен проект

Изпълнителят трябва да изготви системен проект, в който са описани всички изисквания за адаптиране на Системата. 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 бележки, корекции или допълнения от страна на Възложителя, Изпълнителят ги отразява и предоставя на Възложителя с нова версия на документа в срок, не по-късен от [X] работни дни.

6.3. Разработване на софтуерното решение

Етапът на разработка включва изпълнението на следните задачи:

- Разработка съгласно изискванията на настоящата техническа спецификация 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.“

6.4. 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 тестовите, управление на дефектите, регресионна политика, инструменти, логистично осигуряване и други параметри на процеса.

6.5. Внедряване

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

6.6. Обучение

В своето техническо предложение участникът следва да предложи метод и списък с материали за обучение за работа на потребителите на адаптираната за работа с еврото [наименование на информационната система].

В рамките на дейността по адаптиране за работа с еврото се разработва план за обучение, в който се описва наборът от всички дейности по обучение на потребителите на [наименование на информационната система].

За провеждането на обученията Изпълнителят е длъжен да осигури за своя сметка учебни материали и лектори.

Планът за обучение трябва да съдържа минимум следните реквизити:

- списък на всички необходими ресурси за организация и провеждане на обучението;
- места за провеждане на обучението;
- времеви график.

Изпълнителят трябва да организира и да проведе обучения за следните групи потребители на [наименование на информационната система]:

- [Потребителска група 1];
- [Потребителска група ...].

6.7. Гаранционна поддръжка

Изпълнителят трябва да осигури за своя сметка гаранционна поддръжка за период от минимум 24 месеца след приемане в експлоатация на надградените функционалности на [наименование на информационната система] във връзка с адаптирането ѝ за работа с еврото.

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, заложиени 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

При надграждането на Системата с нови модули и/или функционалности, свързани с адаптирането ѝ към въвеждане на еврото в Република България, да бъдат спазвани изложените по-долу изисквания за информационни системи в държавната администрация.

7.1. Интеграция с външни информационни системи

За реализираните основни бизнес процеси и изградени интеграции в реално време на Системата с информационни системи на други администрации е необходимо:

- Изпълнителят да анализира, класифицира и опише в системния проект всички приложни програмни интерфейси (API), изградени в системата, както и съществуващите връзки към други информационни системи;

- Да осъществи необходимите промени в приложните програмни интерфейси (използваните видове web услуги и методи), свързани с адаптиране на системата към въвеждане на еврото;
- След като се изпълнят успешни интеграционни тестове, Изпълнителят следва да изготви технически спецификации за интеграция, характеризираща преработените интерфейси, и да ги предостави на собствениците на външните системи, с които надгражданата система има осъществена интеграция.

7.2. 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
 - ✓ Mozilla Public License 2.0
 - ✓ EUPL (European Union Public License)
- 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 глава шеста, раздел IV „Хранилище за изходен код“ от НОИИСРЕАУ;
- 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.

7.3. Системна и приложна архитектура

- Адаптирането на Системата във връзка с въвеждане на еврото в Република България трябва да бъде реализирано със стандартни технологии и да поддържа общоприети комуникационни стандарти, които ще гарантират съвместимост на Системата с бъдещи разработки и/или надграждания на същата в резултат на законови промени. Съществуващите модулни функционалности трябва да бъдат рефакторирани и/или надградени по начин, който да осигури изпълнението на настоящото изискване;
- Адаптираната информационна система трябва да е максимално параметризирана и да позволява настройка и промяна на параметрите през служебен (администраторски) потребителски интерфейс;
- Задължително наличие и използване на програмни интерфейси, изискуемите метаданни и атрибути за версия, достъпност за стари версии - минимум 24 месеца след публикуване на нова версия, съгласно изискването по чл. 14 и чл. 41 от НОИИСРЕАУ;
- 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 по време на гаранционния период;
- Изпълнителят трябва да създаде административен потребителски интерфейс с функционалност, чрез която може да бъде извършвана конфигурацията на софтуера, в това число избор на валута. Интерфейсът на Системата трябва да предоставя възможност за визуализация на двете валути – лева и евро в преходния период, а след него – само в евро;
- Всеки нов обект, свързан с адаптация на системата за въвеждане на еврото, трябва да има уникален идентификатор, който да се използва включително при интеграция с уебслужби с външни системи.

7.4. 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).
- Промените в публичните модули, които ще предоставят информация и електронни административни услуги в интернет, трябва да отговарят на актуалните уебстандарты за визуализиране на съдържание.

7.5. Информационна сигурност и интегритет на данните

- Да се използва съществуващата система за ежедневно създаване на резервни копия на данните, които да се съхраняват извън инфраструктурата на системата;

- Програмният код трябва да включва методи за автоматична синтизация 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 минималните изисквания за мрежова и информационна сигурност;
- Да се използва съществуващият модул за проследимост на действия и събития в Системата. 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 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.

Изисквания по отношение на киберсигурност в съответствие с чл. 12, ал. 1 от НМИМИС, поставени с цел достигане на изискваното ниво на сигурност на информацията. В мрежите и информационните системи следва да се предвидят следните изисквания:

- Да бъдат включени адекватни и комплексни изисквания за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира, че изискваното ниво на сигурност на информацията, мрежите и информационните системи е заложено още в етапа на разработка и внедряване.
- Да се представят анализ и оценка на риска, които да послужат като основа за включването на адекватни и комплексни изисквания за мрежова и информационна сигурност.
- Ненужните портове по протоколи TCP и User Datagram Protocol (UDP) да бъдат забранени чрез адекватно конфигуриране на използваните софтуерни решения, хардуерни устройства и оборудване за защита и контрол на трафика.
- Да се използва отделна, изолирана от другите информационни и комуникационни системи и от интернет подходящо защитена среда (мрежа, система, софтуер и др.) за целите на администриране на информационните и комуникационните системи и техните компоненти. Тази среда трябва да не се използва за други цели.
- Да се валидират всички входни данни, постъпващи от клиента, включително съдържанието, предоставено от потребителя, и съдържанието на браузъра, като headers на препращащия и потребителски агент.

- Всички данни да бъдат кодирани с HTML, изпращани от клиента и показвани в уебстраница.
- Да се ограничават заявките и по-специално по максимална дължина на съдържанието, максимална дължина на заявката и максимална дължина на заявката по URL.
- Да се конфигурира типът и размерът на headers, които уебсървърът ще приеме.
- Да се ограничава времетраенето на връзката (connection Timeout) - времето, за което сървърът изчаква всички headers на заявката, преди да я прекъсне, както и минималният брой байтове в секунда при изпращане на отговор на заявка:
 - ✓ Да се въведе ограничение на броя неуспешни опити за влизане в системата;
 - ✓ Да не се допуска извеждането на списък на уебдиректориите;
- Бисквитките (cookies) задължително да имат:
 - ✓ флаг за защита (security flag), който инструктира браузъра, че „бисквитката“ може да бъде достъпна само чрез защитени SSL канали;
 - ✓ флаг HTTP only, който инструктира браузъра, че „бисквитката“ може да бъде достъпна само от сървъра, а не от скриптовете, от страна на клиента;
- Да се предвидят и предприемат мерки за защита на DNS, като задължително се прилага DNSSEC (Domain Name System Security Extensions); - не е приложимо – това е вътрешна система, а не публична.
- По отношение на системните записи (Logs) да бъдат предвидени следните възможности:
 - ✓ в сървъри за приложения, които поддържат критични дейности, сървъри от системната инфраструктура, сървъри от мрежовата инфраструктура, охранителни съоръжения, станции за инженеринг и поддръжка на индустриални системи, мрежово оборудване и работни места на администратори се регистрират автоматично всички събития, които са свързани най-малко с автентикация на потребителите, управление на профилите, правата на достъп, промени в правилата за сигурност и функциониране на информационните и комуникационните системи;
 - ✓ за всяко от тези събития в записите се отбелязва астрономическото време, когато е настъпило събитието;
- да бъде предвидена възможност за синхронизиране на часовниците на компоненти на информационните и комуникационните системи, като се използва протокол NTP V4 (Network Time Protocol, версия 4.0 и следващи), основан на RFC 5905 на IETF от 2010 г., като се осигурява хронометрична детерминация с времевата скала на UTC (Coordinated Universal Time), или аналогичен;
- да се предвиди как информацията ще бъде архивирана за срок, не по-кратък от дванадесет месеца.

7.6. Системен журнал

Адаптираната информационна система във връзка с изискванията за въвеждане на еврото е задължително да използва действащия системен журнал към момента на въвеждане на същата в редовна експлоатация, допълнен с новите оперативни необходиминости, предварително детайлизирани в приетия от Възложителя Системен проект (т. 6.2).

7.7. Дизайн на бази данни и взаимодействие с тях

При използване на база данни (релационна или нерелационна (NoSQL) следва да бъдат следвани добрите практики за редизайн и взаимодействие с базата данни, в т.ч.:

- новите имена на полета и колони на съществуващи таблици или нови такива 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;
- 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.

7.8. Специфични изисквания при адаптиране на ИС за работа с евро

При адаптиране на Системата за работа с евро Изпълнителят трябва да спазва специфични изисквания, съобразени с нормативната уредба и принципите, които са взети предвид при въвеждането му в Република България - защита на потребителите, прозрачност, ефективност и икономичност.

В етапа на анализ на данните и изискванията и изготвяне на системен проект Изпълнителят трябва да се съобрази със следните специфични изисквания:

- Превалутирането от левове в евро да се извършва, като числовата стойност в левове се раздели на пълната числова стойност на официалния валутен курс, изразен с шест цифри, с всичките пет знака след десетичната запетая.
- Официалният валутен курс не се закръглява или съкращава при извършването на превалутирането.
- След превалутиране получената сума да се закръглява до втория знак след десетичната запетая на базата на третия знак след десетичната запетая в съответствие със следното математическо правило за закръгляване:
 - а) когато третият знак след десетичната запетая е по-малък от пет, вторият знак след десетичната запетая остава непроменен;
 - б) когато третият знак след десетичната запетая е равен на или по-голям от пет, вторият знак след десетичната запетая се увеличава с една единица.
- Изключение от правилото, на базата на което се извършва закръгляването, се допуска само когато нормативен документ или правен акт на Европейския съюз, предвиждат да се извършва до знак след десетичната запетая, различен от посочения по-горе.
- Стойностите, посочени в левове в съществуващите правни инструменти, при надграждане на ИС да се считат за стойности в евро при прилагане на официалния валутен курс и правилата за превалутиране по чл. 12 и съответно за закръгляване - по чл. 13 на ЗВЕРБ, или по специалните правила за закръгляване, предвидени в ЗВЕРБ.

При надграждане на Системата във връзка с адаптацията ѝ за работа с евро, в периода на двойно обращение на лева и еврото и двойно обозначаване на цените на стоките и услугите в евро и в левове, Изпълнителят трябва да спазва следните изисквания:

- От датата на въвеждане на еврото в Република България за период от един месец официални парични единици на територията на Република България са левът и еврото (период на двойно обращение на лева и еврото), от което следва, че работните процеси, осъществявани чрез Системата, трябва да позволяват действия с двете парични единици. След изтичане на периода левът престава да бъде законно платежно средство на територията на Република България.
- В периода на двойно обозначаване на цените на стоките и услугите в евро и в левове (чл. 15 на ЗВЕРБ) таксите за ЕАУ, предоставяни чрез Системата, се обозначават в левове и в евро, като за таксите в евро се прилагат правилата за превалутиране и закръгляване или специалните правила за закръгляване, предвидени в ЗВЕРБ.
- Периодът на двойно обозначаване на таксите за предоставяните ЕАУ в левове и в евро започва един месец след датата на влизане в сила на Решението за приемането на еврото и приключва 12 месеца след датата на въвеждане на еврото в Република България.
- При двойното обозначаване на таксите за услугите, стойностите в левове и в евро се обозначават в непосредствена близост, изписват се ясно, четливо, недвусмислено и лесно разбираемо, с еднакъв размер на шрифта, по начин, който не въвежда потребителите в заблуждение.
- В периода на двойно обозначаване крайната сума, която се заплаща от потребителя за предоставяна от АО услуга, се обявява в издавания фискален/системен бон в левове и в евро заедно с официалния валутен курс на лева към еврото.
- От датата на въвеждане на еврото в Република България всички плащания през Системата се регистрират и отчитат в евро и евроцентове, като съответните операции се извършват в автоматичен режим.

8. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ДЕЙНОСТИТЕ ПО ПРОЕКТА

8.1. Дейност 1 [Наименование на дейността]

8.1.1. Описание на дейността

8.1.2. Изисквания към изпълнение на дейността

8.1.3. Очаквани резултати

8.2. Дейност ... [Наименование на дейността]

8.2.1. Описание на дейността

8.2.2. Изисквания към изпълнение на дейността

8.2.3. Очаквани резултати

9. ДОКУМЕНТАЦИЯ

9.1. Изисквания към документацията

- Цялата документация и всички технически описания, ръководства за работа, администриране и поддръжка на Системата, включително 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 уебслужби, 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 уебслужба;
- 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 машинночитим 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 изискваната документация по проекта включва следните 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 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)

Приложение	№	3
към	11,	5
чл.	ал.	
(Ново – ДВ, бр. 80 от 2024 г.)		

МЕТОДИКА

за автоматизирано генериране на уникален идентификатор на записи в регистър/регистри съгласно чл. 11, ал. 5 от Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги

Методиката включва правила за автоматизирано генериране на уникален регистров идентификатор, осигуряващ номериране на записите в регистър.

Уникалният регистров идентификатор (УРИ) е 16-цифров стринг от символи с формат: YYXXXDDDDNNNNNC

Описание на УРИ:

YY – последните две цифри от годината;

XXXX – код от Единния бюджетен класификатор (ЕБК) на собственика на системата;

DDD – пореден ден от годината;

NNNNNN – автоматичен инкремент на 6 цифри от: „0“, „1“, „2“, „3“, „4“, „5“, „6“, „7“, „8“, „9“;

C – контролното число е за целия стринг: YYXXXDDDDNNNNNN.

Контролно число се изчислява, като се събират петте трицифрени групи и получената сума се дели по модул 10.

Пример за изчисляване на контролното число на идентификатор: 247500115002459,

където:

YY = 24

XXXX = 7500

DDD = 115

NNNNNN = 002459

$$C = ((247 + 500 + 115 + 002 + 459) \% 10) = 3$$

Уникален регистров идентификатор: 2475001150024593