


ЗАЯВКА по Рамков договор № 100 от 19.12.2023 г. (вх. № ПО-16-3466/19.12.2023 г. на ИО АД)		<input checked="" type="checkbox"/>		
ЗАЯВКА по Рамков договор № 100 от 19.12.2023 г. (актуализирана)		<input type="checkbox"/> ¹		
Позиция от ПГ-2025 г.:	<i>№ по ред от ПГ</i>	346		
Описание на проект съгласно ПГ:	5.3 <i>Комплексна услуга за реализиране на свързаност между основен и резервен център на МФ</i>			
CPV код	72228000-9 <i>Консултантски услуги, свързани с интегриране на хардуер</i> 51611100-9 <i>Услуги по инсталиране на хардуер</i> 72100000-6 <i>Консултантски услуги по хардуер</i>			
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	Рег. № МЕУ-5458/09.04.2026 г.			
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ			
Стойност: (стойността следва да съответства на заложената в План-графика) без ДДС, в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово	<table border="1"> <tr> <td><i>Стойност на проект 5.3, ред 346</i></td> </tr> <tr> <td>14 500, 00 евро</td> </tr> </table>		<i>Стойност на проект 5.3, ред 346</i>	14 500, 00 евро
<i>Стойност на проект 5.3, ред 346</i>				
14 500, 00 евро				
Начин за плащане: (еднократно, на части, периодично, авансово или др.)	Еднократно, след подписан Приемо-предавателен протокол (ППП) между Изпълнителя и Бенефициера по чл. 6 от Договора (Образец №1), удостоверяващ приемане на извършените дейности съгласно Техническите параметри (ТП) към Заявката и издадена фактура, одобрена от Бенефициера.			
Плащане с акредитив или авансово ДА/НЕ	НЕ			
Документи за плащане с акредитив или авансово	Не е приложимо			
Срок на изпълнение: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	до 4 месеца от подписване на заявка			
Гаранционен срок: (от дата – до дата или в месеци, ако не е обвързан с конкретна дата)	Осигуряване безпроблемна работоспособност на реализираната свързаност до 31.12.2026 г.			
Отчитане: (периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)	Еднократно, чрез Приемо-предавателен протокол (ППП) между Изпълнителя и Бенефициера по чл. 6 от Договора (Образец №1), удостоверяващ успешното изпълнение на извършените дейности съгласно Техническите параметри (ТП) към Заявката			
Приложения: (напр: технически параметри, образци на отчетни документи)	<ul style="list-style-type: none"> • ТП за реализиране на свързаност между основен и резервен център в Министерство на финансите; • Образец № 1 – Приемо-предавателен протокол по чл. 6 от Договора между Изпълнителя и Бенефициера. 			
Настоящата заявка да се изпълни при условията на приложените Технически параметри.				
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:				
Ръководител на проект по заявката от страна на МФ (напр: представител на дирекцията – Заявител):		Подпис: 		
ЗАЯВКАТА е ОДОБРЕНА ОТ:				

¹ Отбелязва се в случай че заявката е актуализирана

Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		<i>Подпис:</i>
Ръководител на договора от страна на БЕНЕФИЦИЕРА:		<i>Подпис:</i>
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		<i>Подпис:</i>
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		<i>Подпис:</i>

Забележка: С една заявка могат да се възлагат повече от един проект по ПП, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКИ ПАРАМЕТРИ

ЗА

**КОМПЛЕКСНА УСЛУГА ЗА РЕАЛИЗИРАНЕ НА
СВЪРЗАНОСТ МЕЖДУ ОСНОВЕН И РЕЗЕРВЕН
ЦЕНТЪР В МИНИСТЕРСТВО НА ФИНАНСИТЕ**

април, 2026 г.

1. Съществуващо положение.

1.1 Между Министерството на финансите (МФ) и Държавна агенция „Електронно управление“ (ДАЕУ) е сключено Споразумение за ползване на информационно-комуникационна услуга „Колокация“ - № СПОР-1/11.01.2021 г., изменено и допълнено с Допълнително споразумение № 1/23.12.2022 г., сключено между МФ, Министерството на електронното управление (МЕУ) и „Изпълнителна агенция „Инфраструктура на електронното управление“ (ИАИЕУ), чиято цел е разполагане на защитен център за резервиране на услуги за обезпечаване на наличността на информационните системи и предоставяне на информационно - комуникационна услуга „Колокация“ на МФ и на администрациите на второстепенните разпоредители с бюджет по бюджета на МФ.

1.2 По проекти 5.1 и 5.3 от План-график за 2021 г. към Рамков договор №5/28.01.2021 г. е доставено описаното в Таблица 1 оборудване, предназначено за резервния ИТ център (РИТЦ) на МФ, разположен в обект на ИАИЕУ. Таблицата е отделен документ с ограничено ползване при спазване на принципа „необходимост да се знае“, с ниво на класификация на информацията - 2, TLP-AMBER съгласно изискванията на Наредбата за минималните изисквания за мрежова и информационна сигурност.

1.3 Наличното в МФ оборудване за основния център е описано в Таблица 2 като отделен документ с ниво на класификация на информацията - 2, TLP-AMBER.

1.4 По проект 6.2 част 9 „Проектиране архитектурата на свързаност между основен и резервен център в Министерство на финансите“ от План-график за 2025 г. към Рамков договор № 100/19.12.2023 г., е изготвен документ наречен „Архитектура на свързаност между основен и резервен център в МФ“. Системният интегратор като изпълнител на този проект, не е констатирал необходимост от закупуване на допълнително оборудване и софтуер.

2. Цел.

Реализиране на свързаност на физическо и логическо ниво между основния ИТ център в МФ и защитения център за резервиране на услуги, разположен в специализиран обект със специално предназначение (СОСП), стопанисван от ИАИЕУ, наричан по-долу „резервен ИТ център“ (РИТЦ) за осъществяване на On-line репликация, backup, архивиране на файлове и възстановяване на продуктивната система без загуба на данни.

3. Място на изпълнение.

Сградата на МФ, намираща се в гр. София, ул. „Г. С. Раковски“ № 102 и защитен център, разположен в СОСП.

4. Изисквания към мрежовата и информационната сигурност.

4.1. Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове в областта.

4.2. Във връзка с мрежовата и информационната сигурност на Бенефициера и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

а) гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на услугата и които ще имат достъп до информация и активи, при взаимодействието им със служители на Бенефициера ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС;

б) при предоставяне на Услугата спазва сигурността на информацията на Бенефициера и на МЕУ. За целта, ангажираните от Изпълнителя за предоставяне на услугата лица, в т.ч. и на трети страни, с които Изпълнителят има сключен договор за изпълнение, които ще имат достъп до информация и активи на МФ, подписват Декларации за опазване на информацията (Приложение № 3 към Рамков Договор № ДОГ-100/2023, Образец), които се предават по електронна поща на Бенефициера. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават своевременно по същия ред;

в) осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

г) се задължава да не разпространява информация, станала му известна при и по повод изпълнението на услугата на трети страни без изричното писмено съгласие на Бенефициера.

4.3. Служителите по чл. 20 от Договора, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване:

а) при изпълнението на задълженията си, осъществяват комуникация с ръководителите на проекта и с ръководителите на договора от страна на Бенефициера и Изпълнителя, а при необходимост ескалират възникнал проблем до прекия си ръководител;

б) служителят от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя в т.ч. и на трети страни, с които Изпълнителят има сключен договор за осигуряване изпълнението на услуги по предмета на Договора;

в) при констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за проекта, служителите по чл. 20 от договора от страна на Бенефициера и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок. Резултатите от анализа, както и конкретни решения за осигуряване на сигурността се предоставят на ръководителите на Договора и на проекта.

5. Управление на качеството.

5.1. Изпълнителят следва да създаде организация за управление на качеството при изпълнението на проекта.

5.2. Ръководителят на проекта от страна на Изпълнителя е отговорен за:

а) предоставяне по електронна поща на подписаните декларации за опазване на информацията (по образец - Приложение № 3 към Договора) на ръководителя на проекта от страна на МФ, на служителите по чл. 20 от Договора, както и на дирекция „Информационни системи“ (ДИС);

б) качеството на изпълнение на дейностите по проекта и правилното им разпределение между лицата, ангажирани с изпълнението;

в) наблюдение на процесите по осигуряване на качеството при изпълнение на проекта и предприемане на коригиращи действия в случай на необходимост.

6. Дейности в обхвата на Услугата.

6.1. Изпълнението на проекта започва с изготвяне на План-график, който се съгласува и одобрява в оперативен порядък по имейл от Бенефициера. План-графикът се актуализира при възникнала необходимост, като актуализацията се одобрява оперативно от Бенефициера.

6.2. В обхвата на услугата се включват дейности по конфигуриране и въвеждане в експлоатация на комуникационна свързаност между основен и резервен ИТ център за данни, както и тестово превключване, прехвърляне на ИС, база данни и система за архивиране, както следва:

а) Изготвяне на нов IP адресен план за резервен ИТ център и реализиране на функционални услуги в основен ИТ център (ОИТЦ), работещи с нови IP адреси;

б) Тестово превключване между отделни приложни сървъри, симулирайки отпадане на системи, дори и технически център след преместване на оборудване;

в) Конфигуриране на устройствата за интернет свързаност през предоставена връзка от МЕУ, за да се използват наличните публични IP адреси на МФ;

г) Конфигуриране на DNS записи за публични услуги към доставчик на DNS услуги – Cloudflare;

д) Изграждане на комуникационна мрежа, базирана на избраните нови частни IP адреси, обслужващи нуждите на РИТЦ;

е) Въвеждане в експлоатация на оборудването в РИТЦ;

ж) Синхронизация на системите, включени в процедурата за възстановяване след бедствие, включително необходимите бази данни и системите за архивиране;

Описание на системите, включени в процедурата за възстановяване след бедствие.

№	Система / услуга - име	Приложен	ДБ сървър	Приоритет
1	Файлов сървър	mfshare		висок
2	Мейл сървър	ex1-SE, ex2-SE, azure-srv, new-mhost3, ESA1, ESA2		висок
3	AD услуги - DNS, DHCP, DC	DC2, DC3, DC4, DMZ-DC, ns2, PFSense		висок
4	Модул МДТ и СОИ към ИСО	mdt-ssh mdt-ws-nap mdt-ws-nap-new mdt-web mdt-rdp mdt-rdp-new mdt-esti mdt-fakeweb	mdt-db1 mdt-db2	висок
5	SAP система на МФ	sap-prd SAP Router SAP WebDispatcher	SAP HANA DB	висок
6	ИС за общините - ИСО, ЦРОД към ИСО	websys	sql5	висок
7	СМАРТ, в т.ч. САОД	smart-web smart-lb1 smart-web2	smart-db	висок
8	ИС SDMS	websys	sql4	висок

9	ИС Управление на държавното съкровище УДС	websys, tsrv	sql5, sql4	висок
10	ИСЦК	wa1, websys	sql3	среден
11	АИС Документооборот	web-ais-new, web-ais-comm	sql2	висок
12	ИС Управление на човешките ресурси	wa1	sql4	висок
13	Софтуер за създаване на единна бюджетна класификация НОМИК	websys	sql5	среден
14	Интернет страница на МФ	new-mhost2	new-mhost1	среден
15	ИС Регистър за минималните помощи – ИС РМП	websys	sql5	среден
16	ИС Разплащания с публични средства - ИС РПС	rms593n1, rms593n2, rms593ng-dev, lb1n1	gc1n1, gc1n2, gc1n3	среден
17	ИСФУКВО	websys	sql5	среден
18	Програмен продукт Аладин		sql3	среден
19	Портал за финансова грамотност ПФГ	PFG	PFG	среден
20	Интернет страница „Държавни помощи“	new-mhost2	new-mhost1	среден

Описание на системите и възможните сценарии за превключване между РИТЦ и ОИТЦ

№	Система/услуга - име	Метод и процедурни стъпки
1	Файлов сървър	DFS name space
2	Мейл сървър	Репликация със средства предоставени от самите системи
3	AD услуги - DNS, DHCP, DC	Репликация със средства предоставени от самите системи
4	Модул МДТ и СОИ към ИСО	При различни IP в резервната среда, ще трябва ръчно да се променят
5	SAP система на МФ	Най-оптимално е да се реализира чрез DB репликация, и отделно на приложния сървър. Задължително трябва да се репликират и saprouter и webdispatcher. Ще трябва и ръчна намеса при необходимост от превключване.
6	ИС за общините - ИСО, ЦРОД към ИСО	Необходима е синхронизация на БД и приложен сървър. Синхронизация на БД и при промяна на приложенията деплой на приложенията в двете среди
7	СМАРТ, в т.ч. САОД	Необходима е синхронизация на PostgreSQL БД и приложен сървър. Ще трябва ръчно да се превключва. Ще е необходимо да се уточнят параметрите за достъп до и от външни институции, има трансфери през SFTP
8	ИС SDMS	Трябва да бъде направена схема на репликация на данните.

9	ИС Управление на държавното съкровище УДС	Необходима е синхронизация на БД и приложен сървър. Синхронизация на БД и при промяна на приложенията деплой на приложенията в двете среди
10	ИСЦК	<p>Трябва да бъде направена репликация на базата. Ще трябва да се направи допълнителни инсталации - на app server. Въпрос предвидено ли е и Pantheon, предвид на факта, че ИСЦК прехвърля данни в Pantheon. Нвма проблем ако се сменят IP адресите.</p> <p>1. ИСЦК</p> <ul style="list-style-type: none"> • Базата данни в isck на сървър SQL3 от основия datacenter ще се репликира на сървър в резервния datacenter. Предполагам, че active-passive и ръчен switch-over ще е напълно достатъчно, но както се прецени от ИО/МФ. Предимство е, че няма да има загуба на данни при срив в основия datacenter (или в рамките на няколко секунди/ минути максимум) • Ще е необходима отделна Виртуална машина в резервния datacenter, на която да се инсталира ИСЦК. ИСЦК ще трябва да се държи в актуална версия със съответните конфигурационни настройки за връзка към резервната база данни. Характеристиките на виртуалната машина, за най-лесно може да отговарят на текущ сървър WA1 • При настъпване на срив ще са необходими следните стъпки: <ul style="list-style-type: none"> o Резервната база данни да се switch-не към active o Клиентите ще отворят друг адрес – вместо isck.minfin.bg например isck-backup.minfin.bg (или DNS-ите ще се пренастроят - както прецени ИО/МФ) • Допълнителният сървър, който е за целите на консигнационните звена и е в DMZ зона (на сървър WebSys), вероятно ще трябва да се инсталира на отделен сървър, ако се иска пълна резервираност <p>2. Pantheon</p> <ul style="list-style-type: none"> • Той използва SQL Express база данни на сървър WA1. Това е важно, тъй като репликация се прави по различен начин и с повече ръчна намеса. • Най-лесния начин за синкване ще е през извършване на пълни/ transactionbackup-и в споделена папка и впоследствие възстановяване. Недостатъци: <ul style="list-style-type: none"> o по-голямото време, в което могат да се загубят данни и допълнителната ръчна работа. <p>Все пак това е решение на МФ/ИО как да се постъпи.</p>

		<p>о При възстановяване на свързанността в основния data center данните ще трябва да се върнат ръчно</p> <ul style="list-style-type: none"> • Клиентите на Pantheon ще имат отделна конфигурация за връзка към резервната база данни
11	АИС Документооборот	Прехвърляне към резервен център може да стане ръчно от архив и ръчни промени по мрежови настройки
12	ИС Управление на човешките ресурси	Прехвърляне към резервен център може да стане ръчно от архив и ръчни промени по мрежови настройки
13	Софтуер за създаване на единна бюджетна класификация НОМИК	Необходима е синхронизация на БД и приложен сървър. Синхронизация на БД и при промяна на приложенията деплой на приложенията в двете среди
14	Интернет страница на МФ	Необходима е репликация на базата данни (MySQL) и на файлов storage (rsync). Ще иска различни конфигурации в двете среди. Използва външни ресурси - SMTP сървър, активна директория. Има cron jobs, които пращат писма. Има интеграция с opendata.government.bg
15	ИС Регистър за минималните помощи - РМП	Необходима е синхронизация на БД и приложен сървър. Синхронизация на БД и при промяна на приложенията деплой на приложенията в двете среди
16	ИС Разплащания с публични средства - ИС РПС	Има MySQL в Galera Cluster с три нода и application сървър с два нода. Трябва първо да се репликира базата данни, след това трябва да се копира файловият сторидж (rsync), плюс има опашки, кронове и long running scripts, които преди да се пуснат на другата машина, трябва да се спрат на първата. Опашките трябва да се синхронизират, за да не се случи backup машината да изпълни някоя задача повторно. Има голям обем от данни.
17	ИСФУКВО	Необходима е синхронизация на БД и приложен сървър. Синхронизация на БД и при промяна на приложенията деплой на приложенията в двете среди
18	Програмен продукт Аладин	Прехвърляне към резервен център може да стане ръчно от архив и ръчни промени по мрежови настройки

19	Портал за финансова грамотност ПФГ	Необходима е репликация на базата данни (PostgreSQL) и на файлов сторидж (rsync).
20	Интернет страница „Държавни помощи“	Необходима е репликация на базата данни (PostgreSQL) и на файлов сторидж (rsync).

- з) Провеждане на тестове за превключване към РИТЦ;
- и) Изчистване на възникнали проблеми при тестово превключване;
- й) Възстановяване услуги в ОИТЦ.

7. Управление на риска

7.1. Изпълнителят следва да прави оценка на рисковете, като идентифицира основните рискове, които могат да попречат за качествено изпълнение на проекта. Идентифицираните рискове се оценяват и анализират, като своевременно се предприемат мерки за тяхното минимизиране.

7.2. В хода на изпълнението на проекта, Изпълнителят следи рисковете, като ги оценява, анализира и идентифицира (евентуално) нови рискове, извършва приоритизиране на рисковете на проекта, с предвиждане на мерки за тяхното минимизиране. При настъпване на критични рискове и други рискове, които да водят до отклонение спрямо първоначално очакваните резултати и изпълнение, същите се докладват своевременно по електронна поща на Бенефициера и се включват в отчетните документи.

7.3. При изпълнение на проекта могат да се вземат предвид следните рискове и да се добавят други, според спецификата на системата:

- а) промяна в нормативната уредба, водеща до промяна в информационна или комуникационна система;
- б) затруднена комуникация между лицата на Бенефициера и Изпълнителя, ангажирани с изпълнението по проекта;
- в) ненавременно изпълнение на дейности по проекта от страна на Изпълнителя;
- г) неправилно и неефективно разпределяне на ресурсите (човешки, времеви и финансови) и отговорностите при изпълнението на проекта;
- д) неинформиране на Бенефициера за всички потенциални проблеми, които биха могли да възникнат в хода на изпълнение на проекта.

7.4. При извършване на оценката за всеки риск поотделно се използват следните критерии за извършване на оценката на:

- а) въздействието – ниско или високо;
- б) вероятността – малка или голяма;
- в) категорията – 1/2/3/4 (категорията е резултата от умножението на въздействието по вероятността);
- г) степента на критичност - критичен, висок, среден, нисък.

7.5. Основните рискове са оценени от Системния интегратор при изпълнението на проект 6.2 част 9 от План-графика за 2025 г. „Проектиране архитектурата на свързаност между основен и резервен център в Министерство на финансите“ и са описани в таблицата по-долу. За нуждите на настоящия проект Изпълнителят следва да преразгледа и допълни тези рискове.

Описание на риск	Ниво на риск	Възможно решение
Невъзможна промяна на изходящ код на приложна система	Високо	Възстановяване от архив и ръчни промени по конфигурационни файлове, след превключване към резервен център Или Преминаване към дизайн активен-активен център и закупуване на нужното допълнително оборудване и свързаност между центровете
Невъзможно осигуряване на допълнително трасе	Високо	Като минимално решение е използването на допълнителен 10Gbit порт на наличен комутатор на ЕЕСМ
Невъзможно осигуряване на интернет и запазване на използваните от МФ публични адреси в резервен технически център	Средно	Осигуряване на интернет с достатъчно количество публични адреси – като минимум 32 адреса
Невъзможно възстановяване на услуга при тестово превключване	Средно	Изчистване на проблема Или Приемане на риска, конкретна система да бъде извадена от списъка на системи в резервен център
Повреда на устройство или компонент при транспортиране в резервен център	Ниско	Осигуряване на застраховка при транспорт и подмяна на дефектирало оборудване или компонент
Недостатъчно захранване (мощност) в резервен технически център	Ниско	Преместване на резервен център в друга локация

ПРИЕМО-ПРЕДАВАТЕЛЕН ПРОТОКОЛ*по Рамков договор № ДОГ-100/19.12.2023 г.**(вх. № ПО-16-3466/19.12.2023 г. на „Информационно обслужване“ АД),
сключен между Министерство на електронното управление, Министерството на
финансите и „Информационно обслужване“ АД*

Позиция от ПГ-2026	34б	5.3. Комплексна услуга за реализиране на свързаност между основен и резервен център на МФ
Дата на изпълнение:		

Между:

1. Ръководителя на проекта от страна на Бенефициера - Министерството на финансите (МФ), от една страна и от друга страна

2. Ръководителя на проекта от страна на Изпълнителя - „Информационно обслужване“ АД,

определени поименно в Заявка №..... за възлагането на проекта и на основание чл. 6 от Договора се подписа настоящият приемо-предавателен протокол за изпълнение на описания по-горе проект.

I. С подписването на протокола се удостоверява изпълнението на дейностите, както следва:.....

II. Финансова справка:

Съгласно условията на Заявката и Техническите параметри към нея, заплащането се извършва еднократно, след успешно отчитане на изпълнението и подписване на настоящия приемо-предавателен протокол.

Извършени дейности в обхвата на проекта:	Стойност в евро.
Общо, без ДДС	
Общо, с ДДС	

III. Управление на риска

Възможните рискове при изграждане на свързаност между двата центъра и тяхната оценка са описани в т.7 от ТП. Възникнали в хода на изпълнението критични рискове (ако има).

IV. Предоставяне на документация

Изпълнителят предоставя следната техническа документация:

- Описание на IP адреси,
- Схема на свързаността му двата центъра
- Резултати от проведените тестове за превключване към РИТЦ и направени конфигурационни настройки
- Предоставяне на Low Level Design

V. Приложения към настоящия приемо-предавателен протокол:

(ако има)

След като обсъдиха изпълнението на дейностите, извършени при изпълнение на проекта, Бенефициерът и Изпълнителят по Договора установиха, че проектът е изпълнен качествено, в срок и в пълен обем.

Настоящият приемо-предавателен протокол е изготвен като електронен документ и е подписан от представителите на Бенефициера и Изпълнителя с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис.

За БЕНЕФИЦИЕРА (приел):	За ИЗПЪЛНИТЕЛЯ (предал):
Ръководител проект: (име, фамилия, подпис)	Ръководител проект: (име, фамилия, подпис)