Приложение № 2
към рамков договор № ДГ-СФ-42/24.11.2023

ЗАЯВКА по Рамков договор № ДГ-СФ-42 (ПО-16-3062) от 24.11.2023 г.	☑
ЗАЯВКА по Рамков договор № …….от ……г. (актуализирана)	☐ [1]

Позиция от ПГ-2026 г.:	*№ по ред от ПГ*	*2*
Описание на проект съгласно ПГ:	*Осигуряване на достъп до правно-информационна система СИЕЛА*	
CPV код	*48422000-2*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	*МИДТ-90-03-248/19.06.2026г.*	
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*	*835,96 евро без ДДС*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*	*Еднократно, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ осигуряване на достъп до правно-информационна система СИЕЛА за период от 12 месеца от датата на осигуряване и издадена фактура на стойност 835,96 евро без ДДС*
Плащане с акредитив или авансово ДА/НЕ	*НЕ*
Документи за плащане с акредитив или авансово	*неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*От датата на осигуряване за срок от 12 месеца*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*неприложимо*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*Еднократно, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ осигуряване на достъп до правно-информационна система СИЕЛА за срок от 12 месеца*
Приложения: (*напр: технически параметри, образци на отчетни документи*)	*Технически параметри*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.	
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:	
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр:		

[1] Отбелязва се в случай че заявката е актуализирана

представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
Ръководител на договора от страна на БЕНЕФИЦИЕРА:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, 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

Осигуряване на достъп до правно-информационна система СИЕЛА

1. Обхват

Обхватът на заявката включва:

- Осигуряване на достъп до правно-информационна система СИЕЛА с WEB базиран достъп за период от 12 месеца, считано от датата на осигуряване при следните параметри:

Продукти:	**Брой работни места:**
Норми	50
Практика	50
Процедури	50
Счетоводство	50
Инфо	50
Евро	50
Строител	1
Енергетика	2
GDPR справочник	1

- Ежедневна актуализация през Интернет на всички посочени продукти за целия период;
- Програмните продукти следва да бъдат достъпни през Интернет (NET) чрез потребителско име и парола.

2. [2]Изисквания към мрежовата и информационната сигурност

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 към тях.

2. Във връзка с мрежовата и информационната сигурност на Възложителя/Бенефициера (МИДТ/АДФИ) и в съответствие с чл. 10 от Наредбата за

[2] Изискванията към мрежовата и информационната сигурност са приложими, в случай, че по време на изпълнение на заявката Изпълнителят (подизпълнителите, когато е приложимо) имат достъп до информация и активи на Бенефициера (АДФИ), които са предмет на защита съгласно приложимото законодателство в областта.

минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

(а) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо), които ще имат достъп до информация, системи и активи, при взаимодействие със служители на Възложителя/Бенефициера (МИДТ/АДФИ), спазват изискванията на информацията Закона за киберсигурност (обн. ДВ, бр. 17 от 13.02.2026 г.) и НМИМИС.

(б) При предоставяне на Услугата спазва правилата за сигурност на информацията на Възложителя/Бенефициера (МИДТ/АДФИ). Преди започване на изпълнението всички ангажирани лица (в т.ч. и подизпълнителите, когато е приложимо) подписват декларации за конфиденциалност и спазване на изискванията за сигурност, които се предоставят на Възложителя. При промяна на персонала декларациите се предоставят в срок до два работни дни .

(в) Определя компетентно лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с определеното от Възложителя лице при инциденти, включително за целите на координация по докладване на инциденти съгласно Закона за киберсигурност.

(г) Осигурява адекватни, пропорционални и основани на оценка на риска технически и организационни мерки за сигурност, . включително мерки за превенция, откриване, реагиране и възстановяване при инциденти, съобразени с потенциалното въздействие върху Възложителя.

(д) Поддържа способност за своевременно откриване, регистриране и анализ на инциденти по мрежова и информационна сигурност, включително чрез логване и мониторинг на системите, свързани с предоставяната услуга.

3. Изпълнителят се задължава да не разпространява, предоставя или използва за цели извън изпълнението на договора информация, станала му известна при или по повод изпълнение на Услугата, без изричното писмено съгласие на Възложителя/Бенефициера (МИДТ/АДФИ).

Задължението за конфиденциалност се прилага и спрямо всички подизпълнители и остава в сила и след прекратяване на договора.

4. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване („лица по чл. 10, ал. 2 от НМИМИС“), имат следните права и задължения:

(а) При изпълнение на задълженията си осъществяват оперативна комуникация с лицата, които имат достъп до системите на съответната администрация;

(б) Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането, поддържането и контрола на мерките за мрежова и информационна сигурност, включително от страна на подизпълнителите;

(в) При получена информация за инцидент или риск за сигурността, лицата по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за анализ на: причините за инцидента, оценка на въздействието върху услугата и системите на Възложителя/Бенефициера (МИДТ/АДФИ), определяне

на условия за възстановяване и закриване на инцидента, оценка на риска за целостта, наличността и сигурността на услугата;

(г) При констатирано неспазване на изискванията за сигурност или договорените параметри на услугата, което създава риск за мрежовата и информационната сигурност, лицата по чл. 10, ал. 2 от НМИМИС съвместно с представителите на Възложителя/Бенефициера (МИДТ/АДФИ) и Изпълнителя извършват анализ на несъответствието и изготвят план с конкретни коригиращи и превантивни мерки в определен срок.

5. Изпълнителят е длъжен да прилага процедури за управление на инциденти, които включват минимум:

- своевременно откриване и класификация на инциденти;
- незабавно уведомяване на Възложителя при инциденти със средно или високо въздействие;
- съдействие при докладване на инциденти към компетентните органи съгласно Закона за киберсигурност;
- съхранение на доказателства и логове, свързани с инцидента, при спазване на принципите за интегритет и проследимост.

6. Изпълнителят гарантира прилагането на минимум следните мерки:

- контрол на достъпа на база роли и принцип „необходим минимум“;
- многофакторна автентикация за административен достъп;
- криптографска защита на данни при пренос и съхранение, когато е приложимо;
- централизирано логване и защита на логовете от манипулация;
- редовно управление на уязвимости и прилагане на актуализации;
- резервиране на данни и периодично тестване на възстановяване;

7. Изпълнителят носи пълна отговорност за спазване на изискванията за киберсигурност от всички подизпълнители и доставчици, използвани при изпълнение на услугата.

Изпълнителят осигурява предварителна оценка на риска при използване на външни компоненти, услуги или софтуерни зависимости, включително отворен код, и предприема мерки за ограничаване на риска.