Съфинансирано от Европейския съюз

ПРОГРАМА НАУЧНИ ИЗСЛЕДВАНИЯ, ИНОВАЦИИ И ДИГИТАЛИЗАЦИЯ ЗА ИНТЕЛИГЕНТНА ТРАНСФОРМАЦИЯ

Министерство на електронното управление
Рег. № МЕУ-СИ-Д-5/16.02.2026

Д О Г О В О Р

№ ..... Рег. № РД-11-73/17.02.2026г.

В гр. София, между:

1. МИНИСТЕРСТВОТО НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ, БУЛСТАТ 180680495 с адрес: гр. София 1000, ул. „Ген. Гурко“ № 6, представлявано от Валентин Мундров – министър на електронното управление и – директор на дирекция „Финанси“, наричано по-долу за краткост ВЪЗЛОЖИТЕЛ,

2. МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО, с адрес: гр. София 1000, пл. „Св. Неделя“ № 5, код по Регистър БУЛСТАТ 000695317, представлявано от доц. д-р Силви Кирилов, министър на здравеопазването и – директор на дирекция „БФ“, наричано по-долу БЕНЕФИЦИЕР, и

3. „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД, ЕИК 831641791, със седалище и адрес на управление: гр. София 1504, район Оборище, ул. „Панайот Волов“ № 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, и

-главен счетоводител, наричано по-долу за краткост ИЗПЪЛНИТЕЛ , от друга страна,

трите наричани по-долу за краткост „страни“, като взеха предвид че:

- услугите, предмет на настоящия договор, представляват дейности по системна интеграция, по смисъла на чл. 7с от ЗЕУ;
- съгласно § 45, ал. 1, изр. 1-во от ПЗР към ЗИД на ЗЕУ системната интеграция по чл. 7с от ЗЕУ, в която са включени услуги по изграждане, поддържане, развитие и наблюдение на работоспособността на информационните и комуникационните системи, използвани от административните органи, както и дейности, които осигуряват изпълнението на тези услуги, се извършва от „Информационно обслужване“ АД, в качеството му на публичен възложител;
- на основание § 45, ал. 2 от ПЗР към ЗИД на ЗЕУ съгласно т. 21 от Решение № 727 на Министерския съвет от 2019 г., с последващи изменения и допълнения БЕНЕФИЦИЕРЪТ е определен като административен орган, който при изпълнение на своите

www.eufunds.bg
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

функции, свързани с дейности по системна интеграция, възлага изпълнението на тези дейности на системния интегратор „Информационно обслужване“ АД;

- ВЪЗЛОЖИТЕЛЯТ е контролиращ орган на ИЗПЪЛНИТЕЛЯ по смисъла на чл. 12, Параграф 1 от Директива 2014/24/ЕС.

- Съгласно чл.7г от ЗЕУ Министърът на електронното управление упражнява върху всички административни органи контрол в рамките на бюджетния процес по отношение на разходите в областта на електронното управление и за използваните от тях информационни и комуникационни технологии и разполага с правомощието да издава задължителни разпореждания до административните органи и лицата по чл. 1, ал. 2 относно спазването на изискванията на ЗЕУ (чл. 7и ЗЕУ),

сключиха настоящия Договор („Договора/Договорът“), с който се споразумяха за следното:

I. ПРЕДМЕТ НА ДОГОВОРА И МЯСТО НА ИЗПЪЛНЕНИЕ

Чл. 1. (1) ВЪЗЛОЖИТЕЛЯТ възлага, а ИЗПЪЛНИТЕЛЯТ приема да осигури чрез трето лице, избрано след проведена процедура по реда на Закона за обществените поръчки (ЗОП), изпълнението на услуги по системна интеграция за БЕНЕФИЦИЕРА, попадащи в обхвата на чл. 7с от ЗЕУ, с наименование **„Осигуряване на платформа за разузнаване и проактивно откриване на киберзаплахи в реално време (Threat Intelligence Solution)“ в сектор „Здравеопазване““** във връзка с проект[1] “Повишаване на капацитета за реагиране при инциденти, засягащи информационната и комуникационна сигурност в сектор „Здравеопазване““, финансиран по Програма "Научни изследвания, иновации и дигитализация за интелигентна трансформация", съгласно заложеното в Техническите параметри (Приложение № 1), неразделна част от настоящия договор.

(2) В обхвата на договора се включва **доставка на разширена платформа за данни за анализ на киберзаплахи и Dark Web инциденти, комбинирана с допълнителни сензори и платформа за събиране и корелиране на индикатори (IOCs), представляваща цялостно решение за Управление на разузнаването за заплахи (Threat Intelligence**

[1] *Посочва се наименованието на проекта, финансиран със средства от Европейските фондове при споделено управление*

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Management) и проактивна киберзащита.

(3) В обхвата на договора се включва и гаранционна поддръжка съгласно Техническите параметри (Приложение №1).

(4) ИЗПЪЛНИТЕЛЯТ се задължава да осигури изпълнението на дейностите по ал. 1, ал. 2 и ал. 3 в съответствие с изискванията на Техническите параметри, които са неразделна част от настоящия договор.

(5) ИЗПЪЛНИТЕЛЯТ се задължава да проведе процедурата по ЗОП, предвидена в ал.1, при спазване принципите на свободна и лоялна конкуренция, равнопоставеност, спазване на основните права и недопускане на дискриминация.

Чл. 2. (1) Място на изпълнение на дейностите по договора: гр. София, Министерство на здравеопазването, пл. "Света Неделя" № 5

(2) При необходимост, по време на изпълнение на дейностите в обхвата на договора е възможно дейности, които не са свързани с достъп до информация, представляваща служебна тайна, да бъдат извършвани на място, различно от посоченото в ал. 1.

II. СРОК НА ДЕЙСТВИЕ И ОСНОВАНИЯ ЗА ПРЕКРАТЯВАНЕ

Чл. 3. (1) Договорът влиза в сила от датата на подписването му от страните, с начална дата на изпълнение на дейностите, включени в Техническите параметри, датата на подписване на договор за обществена поръчка между „Информационно обслужване" АД и избран изпълнител по ЗОП и срокове, както следва:

1. Срок за изпълнение на дейностите по чл.1, ал.1 – до 4 (четири) месеца от датата на влизане в сила на договора;
2. Срок за изпълнение на дейностите по чл.1, ал.2 – до 30 (тридесет) работни дни от датата на влизане в сила на договора с избран изпълнител по ЗОП;

3. Срок за гаранционна поддръжка - съгласно Техническите параметри (Приложение №1);

(2) При възникване на непредвидени обстоятелства, вкл. обжалване на решения на ВЪЗЛОЖИТЕЛЯ или на ИЗПЪЛНИТЕЛЯ, посоченият/те в ал. 1 срокове се считат за автоматично продължен/и със срока на действие на съответните непредвидени обстоятелства, за което се изготвя констативен протокол. Констативният протокол се съставя като

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

електронен документ и се подписва от лицата по чл.18, чл.19 и чл.20 от Договора с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис.

Чл. 4. (1) Договорът се прекратява:

1. С изтичане на срока на предоставяне на дейностите по гаранционна поддръжка по чл. 3, ал.1, т. 3 от договора;

2. По взаимно съгласие на страните, изразено в писмена форма;

3. При настъпване на обективна невъзможност за изпълнение на договора, както и при отмяна на правата на системния интегратор за изпълнение на съответните дейности, посредством промяна в нормативната уредба. За избягване на съмнение случаите на изменение на правната уредба включват и приемането на акт от правителството на Република България, който може да уреди по друг начин възлагането на дейността по системна интеграция на настоящия системен интегратор.

(2) В случай, че ИЗПЪЛНИТЕЛЯТ наруши съществено условие на настоящия Договор, и не успее да отстрани нарушението в срок до 30 (тридесет) дни от писмено уведомление за извършеното нарушение, ИЗПЪЛНИТЕЛЯТ е в неизпълнение и ВЪЗЛОЖИТЕЛЯТ има право да развали Договора без предизвестие. При настъпването на всяко „нарушаване на съществено условие по Договора“ от страна на ИЗПЪЛНИТЕЛЯ, се съставя протокол, подписан от лицата по чл. 18, чл.19 и чл.20, определени от страните по Договора за отговарящи за изпълнението му. За „съществено условие” по смисъла на изречение първо се счита такова условие, което е свързано с основните права и задължения на страните по Договора, и чието неизпълнение води до неизпълнение на предмета на Договора.

(3) ВЪЗЛОЖИТЕЛЯТ може по своя преценка да удължи 30-дневния период по ал. 2 за такъв период, за който ИЗПЪЛНИТЕЛЯТ продължава нормалните усилия за отстраняване на неизпълнението.

(4) ВЪЗЛОЖИТЕЛЯТ има право едностранно да прекрати договора:

1. при започване на процедура по ликвидация на ИЗПЪЛНИТЕЛЯ;

2. при откриване на производство за обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ, както и при обявяване в несъстоятелност на ИЗПЪЛНИТЕЛЯ;

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

(5) При прекратяване на Договора, БЕНЕФИЦИЕРЪТ заплаща на ИЗПЪЛНИТЕЛЯ всички суми за дейностите, изпълнени съгласно този Договор, които са били дължими към момента на прекратяването му.

III. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 5. (1) Максимално допустимата стойност за изпълнение на услугата, съгласно предмета на договора по чл. 1, е в размер на 495 000 (четиристотин деветдесет и пет хиляди) евро без ДДС, съответно 594 000 (петстотин деветдесет и четири хиляди) евро с включен ДДС, при действаща 20 % ставка на ДДС. При законодателна промяна в размера на приложимата ставка, възнаграждението се актуализира в съответствие с настъпилото изменение, без необходимост от подписване на допълнително споразумение.

(2) БЕНЕФИЦИЕРЪТ заплаща на ИЗПЪЛНИТЕЛЯ общата стойност за изпълнение на услугата по чл. 1 от договора в размер, съгласно ценовото предложение на избрания изпълнител, определен от „Информационно обслужване“ АД след провеждане на процедура за възлагане на обществена поръчка по реда на ЗОП.

(3) В Цената по ал. 2 са включени всички разходи на ИЗПЪЛНИТЕЛЯ за изпълнение на Услугите, като БЕНЕФИЦИЕРЪТ не дължи заплащането на каквито и да е други разноски, направени от ИЗПЪЛНИТЕЛЯ.

(4) Цената по ал. 2 включва изпълнение на дейностите, посочени в Приложение № 1 към договора.

(5) БЕНЕФИЦИЕРЪТ заплаща на ИЗПЪЛНИТЕЛЯ цената за извършената услуга, предмет на този договор *еднократно*, в срок до 30 (тридесет) дни от получаване на издадена от ИЗПЪЛНИТЕЛЯ оригинална фактура и подписани между ИЗПЪЛНИТЕЛЯ и БЕНЕФИЦИЕРА двустранни приемо-предавателни протоколи (за приемането на резултатите от изпълнението на дейностите по чл. 1, ал. 2 от договора) от ръководителите на договора за двете страни, при спазване на условията по ал. 6.

(6) Плащането по този Договор се извършва въз основа на следните документи:

1. двустранни приемо-предавателни протоколи (за приемането на резултатите от изпълнението на дейностите по чл. 1, ал. 2 от договора), съставени като електронни документи и подписани от ръководителите на договора за ИЗПЪЛНИТЕЛЯ и БЕНЕФИЦИЕРА с електронен подпис, създаден с квалифицирано удостоверение за

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

електронен подпис на БЕНЕФИЦИЕРА и ИЗПЪЛНИТЕЛЯ, придружени от съответните документи - резултати от изпълнението на дейностите по чл. 1, ал. 2 от договора в съответствие с изискванията на Техническите параметри, които са неразделна част от настоящия договор и при съответно спазване на разпоредбите на Раздел VII (Отговорности) от Договора; и

2. фактура, издадена от ИЗПЪЛНИТЕЛЯ, представена на БЕНЕФИЦИЕРА и подписана от ръководителя по договора за БЕНЕФИЦИЕРА.

(7) Преди извършване на плащане от БЕНЕФИЦИЕРА се прилагат правилата на Министерство на финансите за извършване на плащания от разпоредители с бюджет.

Чл. 6. (1) Изплащането на договореното възнаграждение, определено съгласно чл. 5, ал. 2 се извършва по следната банкова сметка на ИЗПЪЛНИТЕЛЯ:

Заличаването на IBAN е на основание чл. 72 и чл. 73 от ДОПК

(2) При промяна на банковата сметка, посочена от ИЗПЪЛНИТЕЛЯ, преди извършване на дължимото плащане, същият уведомява БЕНЕФИЦИЕРА писмено в 3-дневен срок от настъпване на промяната. В случай, че не уведоми БЕНЕФИЦИЕРА в този срок, плащането по посочената в Договора сметка се счита за валидно извършено.

Чл. 7. Страните се съгласяват, че в случай, че съответната коректно издадена фактура не е получена от БЕНЕФИЦИЕРА, няма да е налице забава от страна на БЕНЕФИЦИЕРА за плащане на дължимите суми и не се дължи лихва за забава за периода, с който е забавено представянето на фактурата.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА ИЗПЪЛНИТЕЛЯ

Чл. 8. (1) ИЗПЪЛНИТЕЛЯТ се задължава да изпълни дейностите, предмет на договора, съгласно чл. 1 от същия, при спазване на изискванията, посочени в Техническите параметри – Приложение № 1 към същия.

(2) ИЗПЪЛНИТЕЛЯТ се задължава при подготовка на образеца на ценово предложение към документацията за провеждане на процедурата за възлагане на обществена поръчка по реда на ЗОП да заложи остойностяване на всяка дейност по чл. 1, ал. 2 от договора.

(3) ИЗПЪЛНИТЕЛЯТ се задължава да избере трето лице – изпълнител на дейностите

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

по чл. 1, ал. 2, посредством прилагане на критерий за възлагане „най-ниска цена“.

(4) ИЗПЪЛНИТЕЛЯТ се задължава да осигури чрез изпълнителя по договора, сключен по реда на чл. 112 от ЗОП, гаранционна поддръжка при условията на този договор и приложенията към него.

Чл. 9. (1) ИЗПЪЛНИТЕЛЯТ се задължава да пази поверителна Конфиденциалната информация, в съответствие с уговореното в чл. 21 от Договора. Да опазва и да не разгласява пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена по закон или по силата на Договора информация, която е станала известна при изпълнението на дейностите по чл. 1, ал. 2, като представи декларация по образец – Приложение №2.

(2) При изпълнение на предмета на Договора, посочен в чл. 1, ИЗПЪЛНИТЕЛЯТ се задължава да прилага някои или всички изброени по-долу изисквания, съобразно обхвата на възложената дейност:

а) да спазва изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност;

б) да прилага адекватни мерки за мрежова и информационна сигурност, включително да доказва прилагането им чрез документи и/или провеждане на одити при необходимост;

в) да прилага система за прозрачност на веригата на доставките, като при поискване, трябва да може да докаже произхода на предлагания ресурс/ услуга и неговата сигурност;

(3) При възлагане изпълнението на дейностите на трети лица, ИЗПЪЛНИТЕЛЯТ следва да изисква от същите да прилагат всички, изброени в ал. 2, изисквания, съобразно обхвата на възложената дейност.

Чл. 10 (1) При изпълнение на дейностите по договора ИЗПЪЛНИТЕЛЯТ, неговите подизпълнители и служители се задължават:

1. да спазват политиката, правилата и процедурите по информационна сигурност на БЕНЕФИЦИЕРА;

2. да опазват и да не разгласяват пред трети лица съдържанието на документацията, която е станала известна при изпълнението на този договор, без писменото съгласие на БЕНЕФИЦИЕРА, с изключение на случаите, когато са задължени по закон за това;

3. да опазват и да не разгласяват пред трети лица съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

информация, която е станала известна при изпълнението на този договор;

4. да обработва законосъобразно и добросъвестно лични данни, доколкото тези данни са изрично необходими за целите на изпълнение на поетия ангажимент;

5. да предоставя лични данни на публични органи (държавни и общински), когато такива данни са изискани въз основа на валидно законово основание и по законоустановен за целта ред, като своевременно уведоми за това ВЪЗЛОЖИТЕЛЯ и БЕНЕФИЦИЕРА ;

6. да предприеме всички необходими организационни и технически мерки за осигуряване на целостта и поверителността на данните в случай, че ВЪЗЛОЖИТЕЛЯТ и/или БЕНЕФИЦИЕРЪТ предостави/ят на ИЗПЪЛНИТЕЛЯ достъп до собствени IT активи, документи и данни;

7. да опазват и да не разгласяват пред трети лица информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, както и да не разгласяват, използват или предоставят на трети лица разработена в полза на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор, с изключение на случаите, когато са задължени по закон за това;

8. да спазват вътрешните правила за достъп и режим на работа в сградата/ сградите на БЕНЕФИЦИЕРА;

9. да спазват всички процедури и изисквания на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИАЕРА за работа в информационната инфраструктура на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА;

10. да не осъществяват достъп до компютърни данни в компютърна система без разрешение, да не добавят, променят, изтриват или унищожават компютърна програма или компютърни данни, да не въвеждат компютърен вирус в компютърните системи или мрежи на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА, да не разпространяват пароли или кодове за достъп до компютърна система или до компютърни данни на ВЪЗЛОЖИТЕЛЯ и на БЕНИФИЦИЕРА, от което би могло да последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна;

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

11. да спазват изискванията на Програма "Научни изследвания, иновации и дигитализация за интелигентна трансформация" за популяризиране на проекта, в т.ч. всяка комуникационна дейност, свързана с проекта (включително на конференции, семинари, информационни материали като брошури, листовки, плакати, презентации и т.н., в електронна форма, чрез социални медии и т.н.), всяка инфраструктура, оборудване или основен резултат, финансиран от безвъзмездната помощ, както и всеки отчетен документ (приемо-предавателен протокол, доклад, фактура и т.н.), трябва да показват емблемата на ЕС и да включват следния текст: „Този [въведете подходящо описание, напр. доклад, публикация, конференция, инфраструктура, оборудване, вмъкване на типа резултат и т.н.] е финансиран по програма "Научни изследвания, иновации и дигитализация за интелигентна трансформация";

12. да предоставят - по време на изпълнение на дейностите по договора или след това - всякаква информация, която се изисква при извършване на одити и проверки на място от европейски институции /Европейска Комисия, Европейска сметна палата, Главна дирекция “Европейска служба за борба с измамите“- OLAF, с цел да се провери допустимостта на разходите и правилното изпълнение на дейностите по настоящия договор, съгласно сключеното между БЕНЕФИЦИЕРА и ЕК грантово споразумение.

(2) С оглед изпълнението на задълженията по ал. 1, ИЗПЪЛНИТЕЛЯТ (представляващите го лица), както и лицата, ангажирани с изпълнението на дейностите (екипа на ИЗПЪЛНИТЕЛЯ), представят декларация за опазване на информацията.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ВЪЗЛОЖИТЕЛЯ И НА БЕНЕФИЦИЕРА

Чл. 11. (1) ВЪЗЛОЖИТЕЛЯТ и БЕНЕФИЦИЕРЪТ следва да предоставят на ИЗПЪЛНИТЕЛЯ необходимото съдействие за изпълнение на Договора.

(2) БЕНЕФИЦИЕРЪТ е длъжен да приеме и заплати извършеното от ИЗПЪЛНИТЕЛЯ в съответствие с Договора.

(3) За постигането на резултатите по дейностите, БЕНЕФИЦИЕРЪТ, чрез неговия екип, се задължава да предостави информация за изградената при БЕНЕФИЦИЕРА ИТ архитектура и свързаност на системите, касаещи предмета на договора.

(4) При необходимост, БЕНЕФИЦИЕРЪТ ще осигури условия за провеждане на работни срещи за изпълнението на договора. Местата ще бъдат осигурени на ангажираните от ИЗПЪЛНИТЕЛЯ по ЗОП лица, при съблюдаване на изискванията на Закона за

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

здравословни и безопасни условия на труд (ЗЗБУТ).

(5) БЕНЕФИЦИЕРЪТ се задължава да осигури на ИЗПЪЛНИТЕЛЯ и избрания изпълнител, определен от „Информационно обслужване“ АД след провеждане на процедура за възлагане на обществена поръчка по реда на ЗОП, достъп до сградата на БЕНЕФИЦИЕРА, съгласно вътрешните процедури на БЕНЕФИЦИЕРА за осигуряване на достъп, за целите на изпълнение на дейностите по договора.

(6) БЕНЕФИЦИЕРЪТ се задължава да предостави достъп до необходимите за изпълнение на дейностите по договора ИТ активи, документация и данни, при получаване на обосновано искане от изпълнителя по ЗОП.

(7) За ВЪЗЛОЖИТЕЛЯ и за БЕНЕФИЦИЕРА няма задължение за осигуряване на офис-техника, консумативи и др. Цялото необходимо оборудване, вкл. техническо, програмно и друго за целите на работата на екипа на изпълнителя по ЗОП, следва да бъде осигурено от него. За целите на извършване на работата по Техническите параметри, БЕНЕФИЦИЕРЪТ се задължава да предостави достъп на ИЗПЪЛНИТЕЛЯ и избрания изпълнител, определен от „Информационно обслужване“ АД след провеждане на процедура за възлагане на обществена поръчка по реда на ЗОП, до онази информация, приложения и технологична среда, която е необходима за успешното извършване на работата и при спазване на утвърдените процедури, правила и политики на БЕНЕФИЦИЕРА.

VI. ОБЩИ И СПЕЦИАЛНИ УСЛОВИЯ ПО ЗЗБУТ

Чл. 12 (1) В случаите на осигуряване на работни места, БЕНЕФИЦИЕРЪТ и ИЗПЪЛНИТЕЛЯТ се задължават да осигурят прилагането на правила за съвместно осигуряване на здравословни и безопасни условия на труд за административната сграда, с адрес: гр. София, пл. “Света Неделя” № 5, в изпълнение на разпоредбата на чл. 18 от ЗЗБУТ, както следва:

1. определят задълженията и отговорностите си за осигуряване на здравословни и безопасни условия на труд при работа на работниците и служителите, както и здравословни и безопасни условия за други лица, които се намират в района на мястото на извършване на дейностите по договора;

2. информират своевременно за възможните опасности и рисковете при работа съгласно ЗЗБУТ и действащите вътрешни правила;

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

3. координират дейностите си за предпазване на работниците и служителите от тези рискове;

4. прилагат всички нормативни документи, отнасящи се до спазване на изискванията за ЗЗБУТ.

(2) С възлагане на дейността, БЕНЕФИЦИЕРЪТ и избрания от „Информационно обслужване“ АД изпълнител по ЗОП, следва да поемат следните конкретни задължения за осигуряване на ЗЗБУТ:

1. На служителите на изпълнителя по ЗОП се провежда начален и периодични инструктажи от длъжностните лица, определени за това, съгласно изискванията на Наредба № РД-07-2/2009 г. за условията и реда за провеждането на периодично обучение и инструктаж на работниците и служителите по правилата за осигуряване на здравословни и безопасни условия на труд;

2. БЕНЕФИЦИЕРЪТ следва да запознае служителите на изпълнителя по ЗОП с разработения, съгласно Наредба № 8121з-647/2014 г. за правилата и нормите за пожарна безопасност при експлоатация на обектите, план за пожарна и аварийна безопасност, план за евакуация, схеми за евакуация с обозначение на евакуационните изходи и средствата за пожарогасене и да извърши обучение за евакуация и работа с пожарогасителна техника;

3. БЕНЕФИЦИЕРЪТ предоставя на служителите на изпълнителя по ЗОП информация за рисковете за здравето и безопасността на неговите служители, както и за мерките, които се предприемат за отстраняването, намаляването или контролирането им, при необходимост.

4. Всички останали изисквания по време на изпълнение на дейностите, извън посочените в настоящия документ ангажименти на БЕНЕФИЦИЕРА по отношение на работна среда и условията за работа, ще бъдат допълнително уточнени, след получаване на заявка от страна на изпълнителя по ЗОП, ведно с обосновка на необходимостта за тяхното предоставяне и съгласно възможността от страна на БЕНЕФИЦИЕРА за това.

(3) При необходимост, БЕНЕФИЦИЕРЪТ се задължава да осигури:

1. ползване на стационарни телефони с вътрешна и външна линия, като разговорите се заплащат от изпълнителя по ЗОП въз основа на издадена фактура от БЕНЕФИЦИЕРА;

2. условия за провеждане на работни срещи.

VII. ОТГОВОРНОСТИ

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Чл. 13. (1) При пълно виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи на БЕНЕФИЦИЕРА неустойка в размер на 5 % от максимално допустимата стойност на договора без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 30-дневен срок от уведомяването. За пълно неизпълнение се приема неизвършването на нито една от дейностите, включени в обхвата на договора по чл. 1, ал. 2.

(2) При частично виновно неизпълнение на договора, ИЗПЪЛНИТЕЛЯТ дължи на БЕНЕФИЦИЕРА неустойка в размер на 1 % от максимално допустимата стойност на договора без ДДС, която се заплаща от ИЗПЪЛНИТЕЛЯ в 30-дневен срок от уведомяването. За частично неизпълнение се приема неизвършването на дейност, включена в обхвата на договора по чл. 1, ал. 2.

(3) В случай, че ИЗПЪЛНИТЕЛЯТ е в забава по негова вина, БЕНЕФИЦИЕРЪТ има право да получи неустойка за забавено изпълнение в размер на 0,01 % на ден върху максимално допустимата стойност на договора без ДДС, считано от деня, следващ деня, в който ИЗПЪЛНИТЕЛЯТ е следвало да извърши съответната дейност, но не повече от 1% от максимално допустимата стойност на договора без ДДС.

(4) В случай че е налице забава по вина на ВЪЗЛОЖИТЕЛЯ и/ или на БЕНЕФИЦИЕРА, ИЗПЪЛНИТЕЛЯТ не дължи неустойка за забавено изпълнение.

(5) При констатирано лошо или друго неточно или частично изпълнение или при отклонение от изискванията на БЕНЕФИЦИЕРА, същият има право да поиска от ИЗПЪЛНИТЕЛЯ да изпълни изцяло и качествено, без да дължи допълнително възнаграждение за това. В случай, че и повторното изпълнение на дейността е некачествено, БЕНЕФИЦИЕРЪТ има право да изиска неустойка в размер на 2 % от максимално допустимата стойност на договора без ДДС.

(6) Всяка забава се удостоверява с констативен протокол, подписан от БЕНЕФИЦИЕРА и от ИЗПЪЛНИТЕЛЯ, чрез лицата по чл. 19 и чл. 20.

(7) БЕНЕФИЦИЕРЪТ може да претендира обезщетение за нанесени вреди и/или пропуснати ползи по общия ред, независимо от начислените неустойки, включително при неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за постигане на целите на мрежовата и информационната сигурност.

(8) В случай на извършване на финансови корекции за изпълнението на настоящия договор БЕНЕФИЦИЕРЪТ може да упражни правото си на регресен иск и да предяви

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

претенции за заплащане на неустойка от ИЗПЪЛНИТЕЛЯ в размера на извършената корекция.

Чл. 14. Страните запазват правото си да търсят обезщетение за вреди, ако тяхната стойност е по-голяма от изплатените неустойки по реда на този раздел.

VIII. АВТОРСКИ ПРАВА

Чл. 15. (1) Авторските и всички сродни права и собствеността върху изработени софтуерни продукти, техният изходен програмен код, дизайнът на интерфейсите и базите данни, чиято разработка попада в обхвата на чл. 1, ал. 1 от договора и всички съпътстващи изработката им проучвания, разработки, скици, чертежи, планове, модели, софтуер, дизайни, описания, документи, данни, файлове, матрици или каквито и да било средства и носители и свързаната с тях документация и други продукти, възникват директно за БЕНЕФИЦИЕРА, в пълния им обем, съгласно действащото законодателство, а в случай че това не е възможно ще се считат за прехвърлени на БЕНЕФИЦИЕРА в пълния им обем, без никакви ограничения в използването, изменението и разпространението им и без БЕНЕФИЦИЕРЪТ да дължи каквито и да било допълнителни плащания и суми освен предвидената в договора стойност. ИЗПЪЛНИТЕЛЯТ потвърждава, че Техническите параметри и цялата информация предоставена му от БЕНЕФИЦИЕРА за изпълнение на задълженията му по настоящия Договор, са изключителна собственост на БЕНЕФИЦИЕРА и същият притежава авторските права върху тях, като ИЗПЪЛНИТЕЛЯТ/ третите лица, на които е възложено изпълнението единствено адаптират концепцията на БЕНЕФИЦИЕРА във вид и по начин, позволяващи използването ѝ за посочените по-горе цели, като всички адаптации, направени в изпълнение на този Договор, както и авторските права върху тях остават изключителна собственост на БЕНЕФИЦИЕРА и могат да бъдат използвани по негово собствено усмотрение свободно в други проекти, развивани, или осъществявани от него.

(2) При разработване на софтуер за БЕНЕФИЦИЕРА, настоящият раздел от договора се счита и следва да бъде тълкуван като договор за създаване на обект на авторско право (произведение) по поръчка, съгласно чл. 42 ал. 1 от Закон за авторското право и сродните му права (ЗАПСП), като Страните изрично се съгласяват и споразумяват, че:

1. авторските права върху софтуерните продукти и части от тях, включително имуществените права съгласно раздел II от ЗАПСП и прехвърлимите неимуществени права,

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

съгласно чл. 15 от ЗАПСП ще възникнат и принадлежат изцяло и безусловно на БЕНЕФИЦИЕРА, като ИЗПЪЛНИТЕЛЯТ декларира и гарантира, че те няма да бъдат обременени с каквито и да било тежести, залози, искове, претенции на трети лица, възбрани и други тежести или права на трети лица;

2. ИЗПЪЛНИТЕЛЯТ предоставя на БЕНЕФИЦИЕРА изключителни права по смисъла на чл. 36, ал. 2 от ЗАПСП за използване на Софтуерните продукти и техни елементи, и обектите, изброени в ал. 1 или части от тях, в случай че авторските права върху тях не могат да възникнат директно за БЕНЕФИЦИЕРА.

(3) За избягване на съмнение, Страните потвърждават и се съгласяват, че правата на БЕНЕФИЦИЕРА върху софтуерните продукти и обектите, изброени в ал. 1, включително и изключителното право на ползване по ал. 2, т. 2 обхващат всички видове използване, както е предвидено в ЗАПСП, без никакви ограничения по отношение на срокове и територия, включително, но не само: право на ползване, промяна, изменение, възпроизвеждане, публикуване, разпространение, продажба, адаптиране, прехвърляне, представяне, маркетинг, разпореждане по какъвто и да било начин и с каквито и да било средства в най-широк възможен смисъл и по най-широк възможен начин за целия срок на действие и закрила на авторското право, за всички държави, където това право може да бъде признато. Това право на БЕНЕФИЦИЕРА е без ограничение по отношение на броя на възпроизвеждането, разпространението или представянето и е валидно за всички държави, езици и начин на оперираане. Освен това ИЗПЪЛНИТЕЛЯТ потвърждава и се съгласява, че цялата търговска репутация и ползи, произтичащи от софтуерните продукти ще възникват и принадлежат на БЕНЕФИЦИЕРА и ИЗПЪЛНИТЕЛЯТ няма да има каквито и да било права и/или претенции в това отношение. ИЗПЪЛНИТЕЛЯТ също потвърждава и се съгласява, че няма и не може да предявява претенции по отношение на каквито и да било права на интелектуална собственост върху Софтуерните продукти.

(4) С изброените по-горе задължения, ИЗПЪЛНИТЕЛЯТ следва да задължи и трети лица, на които ще възложи за изпълнение дейностите по настоящия договор да не прехвърлят на други лица каквито и да било права свързани със софтуерни продукти, включително, но не само правото на ползване и/или на промяна, както и нямат право да използват и/или прехвърлят, разкриват или предоставят по какъвто и да било начин на други

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

лица концепцията на БЕНЕФИЦИЕРА, съдържаща се в предоставените Технически параметри или други документи, предоставени по повод изпълнението на договора.

IX. ДРУГИ УСЛОВИЯ

Чл. 16. Всички съобщения, уведомления и документи по изпълнението на настоящия договор се съставят в електронен вид и се подписват с електронен подпис в PDF -формат. Кореспонденцията се извършва чрез електронна поща на електронните адреси, посочени от страните.

Чл. 17. Спорни въпроси, възникнали при действието на този договор се решават по пътя на споразумения, а нерешените се отнасят за решаване от компетентния съд.

Чл. 18. Отговарящ за изпълнението на договора от страна на ВЪЗЛОЖИТЕЛЯ и координатор за времето на неговото действие е - държавен експерт, отдел „Политики, анализи и методология“, дирекция „Дигитална трансформация“, тел. ел. адрес: в нейно отсъствие - - експерт, анализатор на работни процеси I степен в отдел „Архитектурни решения за дигитална трансформация“, дирекция „Дигитална трансформация“, тел. , ел. адрес: , а в нейно отсъствие – началник на отдел „Национален координационен център“, дирекция „Мрежова и информационна сигурност“, тел. , ел. адрес:

Чл. 19. Отговарящ за изпълнението от страна на БЕНЕФИЦИЕРА, наричан ръководител договор за времето на неговото действие, е , системен администратор I-ва степен, Дирекция „Здравно-информационни системи“, тел: , ел. адрес: в негово/нейно отсъствие , Дирекция „Здравно-информационни системи“, тел: , ел. адрес:

Чл. 20. Отговарящ за изпълнението от страна на ИЗПЪЛНИТЕЛЯ, наричан ръководител договор за времето на неговото действие, е , Ръководител сектор, Реагиране при инциденти и управление на заплахи, тел: ел. адрес: а в негово отсъствие , Координатор сигурност,

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Чл. 21. (1) Всяка от Страните по този Договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другите Страни, станала ѝ известна при или по повод изпълнението на Договора („Конфиденциална информация“). Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другите Страни, от каквото и да е естество или в каквато и да е форма, включително, финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни, образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство, свързани с изпълнението на Договора.

(2) Конфиденциална информация за целите на настоящия договор включва и:

1. съдържанието на документацията, която е станала известна при изпълнението на договора;

2. съдържанието на данъчна и осигурителна информация, лични данни и друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на договора;

3. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА, комуникации, мрежи и информационни системи на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА, изготвени в хода на изпълнението документи и/или всякакви други резултати от изпълнението, разработена в полза на БЕНЕФИЦИЕРА или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението нанастоящия договор.

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на Договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и действащата нормативна уредба.

(4) С изключение на случаите, посочени в ал. 5 на този член, Конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другаите Страни, като това съгласие не може да бъде отказано безпричинно.

(5) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. информацията е станала или става публично достъпна, без нарушаване на този Договор от която и да е от Страните;

2. информацията се изисква по силата на закон, приложим спрямо която и да е от Страните; или

3. предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната Страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 Страната, която следва да предостави информацията, уведомява незабавно другите Страни по Договора.

(6) Задълженията по този член се отнасят до ИЗПЪЛНИТЕЛЯ, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, като ИЗПЪЛНИТЕЛЯТ отговаря за изпълнението на тези задължения от страна на такива лица.

(7) Задълженията, свързани с неразкриване на Конфиденциалната информация остават в сила и след прекратяване на Договора на каквото и да е основание.

(8) ИЗПЪЛНИТЕЛЯТ няма право да дава публични изявления и съобщения, да разкрива или разгласява каквато и да е информация, която е получил във връзка с извършване на дейностите, предмет на този договор, независимо дали е въз основа на данни и материали на ВЪЗЛОЖИТЕЛЯ и/или на БЕНЕФИЦИЕРА или на резултати от работата на ИЗПЪЛНИТЕЛЯ, без предварителното писмено съгласие на ВЪЗЛОЖИТЕЛЯ и на БЕНЕФИЦИЕРА, което съгласие няма да бъде безпричинно отказано или забавено.

---------- www.eufunds.bg ----------
"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

X. НЕПРЕОДОЛИМА СИЛА

Чл. 22. (1) Страните не отговарят за неизпълнение на задължение по този Договор, когато невъзможността за изпълнение се дължи на непреодолима сила. За целите на този Договор, „непреодолима сила“ има значението на това понятие по смисъла на чл. 306, ал. 2 от Търговския закон.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другите Страни в срок до 3 *(три)* дни от настъпване на непреодолимата сила. Към уведомлението се прилагат всички релевантни и/или нормативно установени доказателства за настъпването и естеството на непреодолимата сила, причинната връзка между това обстоятелство и невъзможността за изпълнение, и очакваното времетраене на неизпълнението.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира, като страните подписват протокол, в който удостоверяват началната дата на спиране. Засегнатата Страна е длъжна, след съгласуване с насрещната Страна, да продължи да изпълнява тази част от задълженията си, които не са възпрепятствани от непреодолимата сила.

(4) След отпадане на непреодолимата сила, засегнатата страна в срок до 3 *(три)* дни уведомява писмено другите страни, като прилага всички релевантни и/или нормативно установени доказателства за отпадането й. Страните подписват протокол, с който удостоверяват датата, от която се възобновява изпълнението на задълженията.

(5) Не може да се позовава на непреодолима сила Страна:

1. която е била в забава или друго неизпълнение преди настъпването на непреодолима сила;

2. която не е информирала другите Страни за настъпването на непреодолима сила; или

3. чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на Договора.

(6) Липсата на парични средства не представлява непреодолима сила.

Настоящият договор е изготвен като електронен документ и влиза в сила след подписването му с квалифициран електронен подпис от представителите на страните, като

---------- www.eufunds.bg ----------
“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

приложенията са негова неразделна част.

Приложения:

1. Приложение № 1 – Технически параметри;
2. Приложение № 2 – Образец на декларация за опазване на информацията.

ЗА ВЪЗЛОЖИТЕЛЯ:

ВАЛЕНТИН МУНДРОВ

МИНИСТЪР НА ЕЛЕКТРОННОТО УПРАВЛЕНИЕ

ЗА ИЗПЪЛНИТЕЛЯ:

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР
НА „ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

ДИРЕКТОР НА ДИРЕКЦИЯ ФИНАНСИ

ГЛАВЕН СЧЕТОВОДИТЕЛ

ЗА БЕНЕФИЦИЕРА:

ДОЦ. Д-Р СИЛВИ КИРИЛОВ
МИНИСТЪР НА ЗДРАВЕОПАЗВАНЕТО

ДИРЕКТОР
НА ДИРЕКЦИЯ „БФ“

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

www.eufunds.bg

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

ТЕХНИЧЕСКИ ПАРАМЕТРИ
за предоставяне на услуги по системна интеграция за „Осигуряване на платформа за разузнаване и проактивно откриване на киберзаплахи в реално време (Threat Intelligence Solution)“ в сектор „Здравеопазване““

I. ЦЕЛ

Настоящите технически параметри имат за цел да дефинират изискванията относно обхвата и изпълнението на дейностите по осигуряване на Платформа за разузнаване и откриване на заплахи (Threat IntelligenceSolution) – решение, което предоставя изпреварваща информация за готвени атаки (фишинг, компрометирани акаунти от организацията, търговия с уязвимости и др.) към организациите и постоянно наблюдение на информационния поток за развиващи се кибер заплахи в реално време (Платформата).

Платформата ще осигури информация и интелигентни анализи на потенциалните рискове, използвайки аналитични инструменти и технологии, за да събира и анализира огромни обеми от данни от различни източници в реално време.

Платформата ще позволи откриването на тенденции, връзки и индикатори на компрометиране, които да бъдат използвани за повишаване на капацитета за реагиране при инциденти, засягащи информационната и комуникационна сигурност в сектор „Здравеопазване“ за нуждите на Министерството на здравеопазването (МЗ) по проект: „Повишаване на капацитета за реагиране при инциденти, засягащи информационната и комуникационна сигурност в сектор „Здравеопазване““, финансиран от програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021 – 2027 г., съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

II. ОБХВАТ

В обхвата на проекта са включени доставки на следните софтуерни продукти:

1. Платформа за анализ на киберзаплахи и Dark web мониторинг

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
REQ. 1.	Предложената разширена платформа за данни за анализ на киберзаплахи и dark web инциденти трябва да включва1 брой лиценз за платформа за Dark Web мониториране, 1 брой лиценз за платформа за разследване на киберинциденти, 1 брой лиценз за достъп до API интерфейс за интеграция с трети решения, всички с валидност и включена поддръжка до 14.04.2028г.
REQ. 2.	Предложеното решение трябва да предоставя платформа за заявки за извършване на търсения за информация за заплахи по IP адрес/домейн/хеш,

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
	имейл, URL адрес и ключови думи, с възможност за интегриране с вътрешни системи и поставяне на съответна оценка на риска.
REQ. 3.	Платформата трябва да предоставя по-задълбочени анализи, като например информация за Jarm Hash, Header Hash, Whois данни, DNS записи и SSL сертификати, за извършване на разследвания, базирани на домейни.
REQ. 4.	Платформата трябва да позволява извършване на търсения в над 50 източника, като например платформи за съобщения, платформи за социални медии, пазари на тъмната мрежа, източници на данни за заплахи, платформи за събиране на API данни и хранилища за код, без езикови ограничения. Платформата трябва да поддържа реномирани източници като Discord, BlueSky, Github GIST, Repo Activity и Huggingface.
REQ. 5.	Платформата трябва да предоставя опция за запазване на специализирани и персонализирани търсения със специфични параметри, които да могат да се изпълняват на редовни интервали. Платформата трябва да предлага разширени възможности за търсене, позволяващи на потребителите да съставят заявки с логически оператори (напр. И, ИЛИ, НЕ) за по-прецизно извличане на данни.
REQ. 6.	Платформата трябва да предлага графичен интерфейс, който да може да предоставя информация за най-новите и критични уязвимости, класифицирани по платформи и доставчици, заедно с оценка на риска от дадени тенденции за уязвимости, а не само за откритите уязвимости в организацията.
REQ. 7.	Данните за уязвимостите следва да включват ключова информация, като например разбивка на CVSS, глобално въздействие, обвързване със зловредни лица и групировки, публично достъпен POC, свързани правила за търсене на заплахи, подробен жизнен цикъл на уязвимостите и свързани IOC индикатори.
REQ. 8.	Платформата трябва да притежава и собствен механизъм за оценяване, базиран на данни от тъмната мрежа, социалните медии, хранилища на код, новини и EPSS оценка, което помага на анализаторите да предвидят вероятността от експлоатация на дадени софтуерни уязвимости.
REQ. 9.	Платформата трябва да предоставя функция за търсене на информация, за да може да локализира специфични уязвимости и да предоставя ключова информация.
REQ. 10.	Платформата трябва да позволява на потребителите да се абонират за конкретни доставчици, услуги, продукти и версии, за да се следят критичните и zero-day уязвимости за тях.
REQ. 11.	Платформата трябва автоматично да може да маркира най-новите и силно критични уязвимости, които се експлоатират активно или са част от ransomware кампании.
REQ. 12.	Платформата трябва да предоставя възможност за откриване на инциденти с изтичане на данни и да има възможност за търсене на информация, свързана с инцидентите, използвайки параметри като домейн, идентификатор на крадеца, URL адрес и потребителско име. Трябва също така да се предоставят опции за филтриране на инциденти, които са използвали данни за вписване на клиенти/служители на организацията.
REQ. 13.	Платформата трябва да може да запазва в лог файлове всички данни,

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
	свързани с инциденти за изтичане на информация, включително възможни зловредни клиенти или служители на организацията, IP адреси, HWID, GUID, потребителско име, пароли, хешове на пароли, NTLM хешове, файлови дървета, семейство на Stealer процеси, информация за машината, операционна система, потребителско име на машината, държава, път на зловредния софтуер, часова зона, тип UAC, антивирусна информация.
REQ. 14.	Платформата трябва да притежава над 130 канала с източници на данни за заплахи от OSINT, както и от собствени източници и източници на трети страни, които трябва да могат да бъдат експортирани в различни формати, минимално JSON, CSV, RAW, TEXT, както и да са достъпни чрез Endpoint API, MISP сървър и TAXII сървър.
REQ. 15.	Данните за заплахи трябва да предоставят 75 000 или повече нови IOC индикатори дневно, включително IP адреси на ботнет мрежи, IP адреси на сървъри за командване и контрол, фалшиви имена на домейни, IP адреси, свързани с APT участници, хешове на известни злонамерени софтуери.
REQ. 16.	Платформата трябва да притежава възможност за експортиране на филтрирани IOC индикатори в SIEM/SOAR/Firewall системи за автоматизирано блокиране на DDOS атаки, усилени DNS атаки и фишинг атаки.
REQ. 17.	Платформата трябва да притежава капацитет да предоставя висококачествени потоци с данни за заплахи за специфични сектори, региони и текущи глобални кампании свързани с кибератаки.
REQ. 18.	Платформата трябва да предоставя възможност за извършване на задълбочено разследване, базирано на IOC индикатори, което да помага на анализаторите да прегледат произхода на злонамерените лица, модели на поведение, визуализиране на взаимоотношенията между IOC индикаторите и възможност за извършване на исторически анализ.
REQ. 19.	Платформата трябва да може да проследява публикации във форуми на нападатели, както и в сайтове, свързани с изтичане на данни, като да позволява филтриране по държава, индустрия, злонамерено лице и категория.
REQ. 20.	Платформата трябва да предоставя опция за извършване на анализ за наличие на зловреден софтуер в над 100 файлови формата, генерирайки подробен аналитичен отчет въз основа на параметри като тип maldoc, използвани IOC, вградени файлове и всякакви подозрителни кодове, открити в качения файл.
REQ. 21.	Платформата трябва да предлага специален изглед с детайлни данни по Mitre ATT&CK рамковия модел. Трябва да се поддържат повече от 35 000 YARA, Sigma, SNORT и SURICATA правила.
REQ. 22.	Платформата трябва да предоставя информация за текущите заплахи, свързани с организацията. Платформата трябва да включва ключова информация, като например водещи злонамерени групировки, които могат да атакуват организацията, както и своевременно да може да докладва за всички уязвимости, активно използвани от тези групировки.
REQ. 23.	Платформата трябва да може активно да наблюдава зловредните групировки и да предоставя актуална информация за тях въз основа на критерии като таргетирана индустрия, държава или други избрани

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
	параметри.
REQ. 24.	Платформата трябва да може да предоставя ежедневни актуализации за новостите около избрани от клиента злонамерени групировки, като трябва да могат да се изпращат автоматично по имейл, обхващайки активности в социални медии, deep web и новинарски източници.
REQ. 25.	Платформата трябва да предоставя директен достъп и чрез API до текущи IOC индикатори, TTP базирани на MITRE ATT&CK рамковия модел, както и информация от YARA-Sigma правила за избрани злонамерени групировки.
REQ. 26.	Платформата трябва да може да предоставя съвети за стратегии за смекчаване на щети и отстраняване на последици за всяка злонамерена групировка, за да може организацията да се подготви предварително срещу потенциални атаки.
REQ. 27.	Платформата трябва да предоставя ключова информация за паричното въздействие на конкретни злонамерени групировки, като например изчисления на финансови печалби, използвани блокчейн адреси, история на финансови транзакции. Трябва да могат да се откриват взаимовръзки между новини, хакерски кампании и конкретни злонамерени групировки.
REQ. 28.	Платформата трябва да може да съпоставя IOC индикатори с наблюдавани кампании за кибератаки, предлагайки допълнителна информация за методологията на реално използвани злонамерени процеси.
REQ. 29.	Платформата трябва да поддържа контекстуално обогатяване на данни за злонамерени лица (напр. псевдоними, геолокация, таргетирани организации, исторически атаки и свързан зловреден софтуер).
REQ. 30.	Платформата трябва да включва изгледи с данни по вертикали като финанси, здравеопазване и правителствени структури, за да се опрости наблюдението на заплахите по сектори.
REQ. 31.	Платформата трябва да позволява изтегляне и преглед на глобални доклади за заплахи, както и собствени доклади за заплахи с опции за филтриране въз основа на сектор, държава, злонамерено лице.
REQ. 32.	Платформата трябва да може да наблюдава милиони компании от трети страни и четвърти страни, ако данните им са достъпни, като да може да извършва задълбочени анализи на глобални тенденции, за да генерира ранни предупредителни сигнали, когато доставчик от трета страна претърпи пробив в сигурността, подкрепени от данни за инциденти от dark web или от публични данни за инциденти.
REQ. 33.	Платформата трябва да може да предоставя информация за глобални тенденции при трети доставчици на услуги на организацията, позволявайки търсене в реално време въз основа на домейн, име на компания, вид атака, сектор и държава, за да се локализират скорошни кибератаки, атаки с криптовируси, атаки с IoT и уеб-базирани атаки срещу доставчиците.
REQ. 34.	Платформата трябва да позволява сканиране за въведени ключови в дълбоката и в тъмната мрежа.
REQ. 35.	Платформата трябва да позволява въвеждането на различни ключови думи, IP адреси, домейни, DLP идентификатори, VIP акаунти, BIN номера за търсене в различни източници на данни.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
REQ. 36.	Платформата трябва да позволява идентифицирането на чувствителни данни чрез използването на DLP идентификатори като IBAN, номер на социално осигуряване, ДДС номер или общи идентификатори и незабавно да генерира аларми в случай на потенциални инциденти с изтичане на данни или инциденти с неоторизирано споделяне на данни.
REQ. 37.	Платформата трябва да позволява преглед на информация за ботнет мрежи, инциденти с лични данни, подозрително съдържание, информация за търгуване с данни на организацията на черния пазар и съдържанието на текстови съобщения от приложения за комуникация в dark web свързани с инциденти.
REQ. 38.	Платформата трябва да предлага достъпен за анализатори архив от исторически споменавания в тъмната мрежа, организирани по зловредно лице, конкретен форум и критичност, за целите на разследване.
REQ. 39.	Платформата трябва да предоставя лесна опция за изтегляне на данните открити в тъмната мрежа чрез имейл съобщения.
REQ. 40.	Платформата трябва да може да открива зловреден софтуер, като например софтуер за кражба на информация, таргетиращ служителите и клиентите на организацията.
REQ. 41.	Платформата трябва да предоставя чрез графичен интерфейс лесното закупуване на данни, предлагани за продажба на черния пазар. Събраните данни трябва да включват информация за засегната машина и нейната конфигурация.
REQ. 42.	Платформата трябва да предоставя чрез графичен интерфейс предварителен преглед на изтекли данни, предлагани за продажба на черния пазар, преди да бъдат закупени.
REQ. 43.	Платформата трябва да може да прави разлика между лична и корпоративна употреба на данни за вписване (чрез съпоставяне на домейни или поставяне на тагове).
REQ. 44.	Платформата трябва да може да проверява за изтекли VPN акаунти и акаунти на служители, които се продават незаконно.
REQ. 45.	Платформата трябва да може да открива и генерира предупреждения за изтичане на идентификационни данни на служители, открити в Telegram канали, хакерски форуми и инциденти с изтичане на данни от трети страни.
REQ. 46.	Платформата трябва да може да открива и докладва за комуникация по канали на зловредни лица от Telegram, Discord сървъри, IRC и ICQ канали, насочени към организацията.
REQ. 47.	Платформата трябва да извършва проверки за подозрително съдържание, свързано с организацията, във форуми за хакери, XSS форуми, форуми за Exploit.in, Pastebin.pl, Paste Sites и да може да генерира аларми при откриване на съдържанието.
REQ. 48.	Платформата трябва да позволява извличане на примерни данни от публикации в тъмната мрежа, при условие че данните са безплатни и могат да бъдат изтеглени.
REQ. 49.	Платформата трябва да може да генерира аларми, когато имейл адресите на VIP акаунти бъдат компрометирани, както и да може да посочва източника на атаката в алармите.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
REQ. 50.	Платформата трябва да поддържа добавянето както на официален, така и на личен имейл адрес на VIP акаунт за наблюдение.
REQ. 51.	Платформата трябва да може да открива изтичане на данни за кредитни и дебитни карти за конфигурирани BIN номера.
REQ. 52.	Достъпът до уеб интерфейса на решението трябва да бъде защитен (чрез HTTPS), като да се поддържа двуфакторна автентикация с SMS, приложение за удостоверяване или чрез имейл удостоверяване.
REQ. 53.	Достъпът до уеб интерфейса на решението трябва да е възможен само от IP адреси, посочени от организацията (да се поддържа изграждането на бял списък с приложения) и трябва да бъде блокиран за други IP адреси.
REQ. 54.	Платформата трябва да има собствено мобилно приложение за iOS и Android, което да позволява на потребителите да управляват платформата директно от мобилните си устройства с достъп до данни от аларми.
REQ. 55.	Платформата трябва да осигурява вграден чатбот, базиран на изкуствен интелект, който да помага на анализаторите с ежедневните операции, като предоставя помощ в реално време.
REQ. 56.	Платформата трябва да предоставя генерирани от изкуствен интелект обобщения за информация, събрана от тъмната мрежа, уязвимости и аларми.
REQ. 57.	Платформата трябва да поддържа персонализирано маркиране на набори от данни, което да позволи безпроблемна интеграция с инструменти на трети страни и платформи за автоматизация, като например SOAR. Чрез SOAR интеграция, платформата трябва да може да уведомява Active Directory за автоматично нулиране на изтекли пароли.
REQ. 58.	Платформата трябва да предоставя секция за управление на аларми, която може да действа като табло за управление на инциденти, предоставяйки възможност за промяна на тежестта на алармите, присвояване на етикети, разпределяне на аларми към членове на екипа с точно проследяване.
REQ. 59.	Платформата трябва да позволява групово активиране и деактивиране на аларми с опции за получаване на аларми чрез имейл съобщения и чрез API интеграции.
REQ. 60.	Генерираните аларми в платформата, в зависимост от инцидентите, трябва да включват информация за източника на изтичането на данни, данни за използваните пароли и линк за достъп до изтеклите данни в суров формат.
REQ. 61.	Платформата трябва да може да съпоставя алармите със съответни стандарти за съответствие (NIST, ISO 27001-2, ISO/IEC 27001, SOC2, NERC, HIPAA, GDPR, FISMA, SOX, PCI DSS, CCPA) и да може да предоставя препоръки за ответни мерки.
REQ. 62.	Платформата трябва да предоставя възможност за добавяне на политики за пароли на организацията в REGEX формат, за да се позволи премахването на фалшиви положителни резултати при различни сигнали за изтичане на идентификационни данни, без да се изисква ръчна намеса.
REQ. 63.	Платформата трябва да предоставя функция за скриване на чувствителни данни, пароли в чист текст и съдържание на лог файлове от анализаторите на решението.
REQ. 64.	Платформата трябва да предоставя опция за абонамент за различни разузнавателни данни, като например ежедневни обобщения на събития,

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
	доклади за заплахи, HUMINT информация.
REQ. 65.	Платформата трябва да позволява собствено одитиране на всички потребители, което позволява проследяване на опитите за влизане в платформата и извършените промени, направени в различни модули/секции, като информацията трябва да може да се съхранява за поне 6 месеца назад.
REQ. 66.	Платформата трябва да поддържа експортиране на потребителски и одитни лог файлове в стандартни формати (Excel) за експортиране и интегриране в SIEM системи.
REQ. 67.	Платформата трябва да предоставя възможност за контрол на достъпа, базиран на роли (RBAC), за да позволи на потребителите да бъдат групирани по роля, функция или оторизация, което може да се персонализира на детайлно ниво.
REQ. 68.	Продуктът трябва да осигурява SSO интеграция чрез използването на SAML протокол за SSO доставчици като ADFS, Microsoft Entra ID, Okta, Google Workspace.
REQ. 69.	Платформата трябва да предоставя графичен уеб-базиран интерфейс, съвместим с всички интернет браузъри, без да изисква допълнителни плъгини, като трябва да може да се актуализира в реално време.
REQ. 70.	Платформата трябва да предоставя различни отчети/доклади по заявка, които могат да бъдат изтеглени от платформата. Отчетите трябва да са достъпни за различни екипи в зависимост от изискванията, като например: - Доклади за нетехническа изпълнителна аудитория, включително брифинги на високо ниво - Доклади за техническа ръководна аудитория с информация за регионални заплахи и заплахи, свързани с индустрията. - Доклади за инциденти за екипи от SOC анализатори - Отчети за отворени портове и уязвимости.
REQ. 71.	Отчетите трябва да са достъпни по заявка или по зададен график в минимално следните формати: CSV, Excel и PDF.
REQ. 72.	Отчетите трябва да могат да се изпращат автоматично на определени интервали, например седмично или месечно, или в определени дни от седмицата до посочени имейл адреси.
REQ. 73.	Платформата трябва да разполага с готови възможности за интеграция с водещи технологии за сигурност като SIEM, SOAR, EDR, защитна стена и други.
REQ. 74.	Платформата трябва да предоставя необходимия скрипт/код за интеграция с водещи технологии за сигурност и трябва да поддържа техните вградени приложения за интеграция.
REQ. 75.	Платформата трябва да осигурява възможност за изпращане на всички генерирани от нея сигнали до съществуващите технологии за сигурност на организацията чрез API интеграция.
REQ. 76.	Платформата трябва да предоставя усъвършенстван двупосочен API интерфейс за обмен на данни със SOAR технологии.
REQ. 77.	Платформата трябва да поддържа Webhooks за интеграция в реално време с платформи за сътрудничество като Slack и MS Teams чрез автоматизиране на доставянето на персонализирани предупреждения.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за анализ на киберзаплахи и Dark web мониторинг	
REQ. 78.	Платформата трябва да позволява задаване на филтри/правила за контрол на това кои аларми или набор от данни се изпращат чрез интеграция с други решения (напр. само критични предупреждения или информация от специфични модули).
REQ. 79.	Платформата трябва да предоставя API-базирани опции за експортиране на данни от заплахи към инструменти за сигурност в обширни формати като Raw Text, Text, Excel, Comma Separated, JSON, TAXII.
REQ. 80.	Платформата трябва да има вградена интеграция с OpenCTI, за да позволи приемането на данни за заплахи.
REQ. 81.	Платформата трябва да предоставя услуга, съвместима с TAXII 2.1, за споделяне на стандартизирани данни (STIX) между инструменти за сигурност.
Гаранция и поддръжка:	
REQ. 82.	Период на поддръжка: до 14.04.2028г.
REQ. 83.	Тип поддръжка: 24x7x365
REQ. 84.	Възможност за актуализиране на софтуера в периода на поддръжката до последна актуална версия на производителя.

2. **Първи слой сензор за анализ на киберзаплахи, свързани с проверка на спам, реклами и фалшиви съобщения в имейл поток**

Минимални технически изисквания за първи слой сензор за анализ на киберзаплахи свързани с проверка на спам, реклами и фалшиви съобщения в имейл поток	
REQ.1	Да извършва последователна проверка на входящи и изходящи email съобщения с различни системи и методи: DKIM и SFP проверка. Филтриране на входящи съобщения на база нивото на репутация на изпращача. Защита против спам с възможност за пропускане, унищожаване, връщане или поставяне на съобщението под карантина. Антивирусна защита. Graymail защита с принудително отстраняване на URL линка за отписване. Подправени съобщения
REQ.2	Да поддържа създаването на политики за прилагане на следните действия върху email съобщенията – пропускане, унищожаване, връщане обратно, поставяне на карантина.
REQ.3	Да поддържа лимитиране броя на изходящите съобщения за всеки потребител.
REQ.4	Да има възможност за поддържка на вградена DLP система.
REQ.5	Да има възможност за интеграция с външна DLP система.
REQ.6	Да поддържа задължително прилагане на договорено TLS шифроване за групи от изпращачи. При получаване на нешифровано съобщение от тези групи, системата трябва да може да върне автоматичен мейл със съобщение, че се използва нешифрована комуникация.
REQ.7	Да има възможност за Envelop Encryption.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за първи слой сензор за анализ на киберзаплахи свързани с проверка на спам, реклами и фалшиви съобщения в имейл поток	
REQ.8	Да поддържа S/MIME шифроване.
REQ.9	Да поддържа създаването на политики и правила за филтриране.
REQ.10	Функционалност за локална карантина.
REQ.11	Функционалност за одитни записи.
REQ.12	Функционалност за доклади.
REQ.13	Да поддържа минимум следните методи за управление и наблюдение: Web базиран графичен интерфейс HTTP и HTTPS Ping DNS FTP NTP SSHv2 WEB API за интеграция с външни системи. Вградена система за изготвяне на отчети.
REQ.14	Софтуерът да е окомплектован със съответните лицензи и права за използване според условията на производителя за минимум 500 лицензa за M3
REQ.15	Възможност за инсталиране върху виртуални или хардуерни устройства или сървъри, съгласно изискванията на производителя.
REQ.16	Ако предложението на участника в обществената поръчка включва сървъри, то те трябва да се доставят с всички необходими лицензи за операционни системи, бази данни и допълнителен софтуер, съгласно изискванията на производителя.
REQ.17	Да поддържа инсталиране върху виртуалните устройства съвместими с VMWare ESXi инфраструктура.
Гаранция и поддръжка:	
REQ.18	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.19	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ.20	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 3 (три) години.

3. **Втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток**

Минимални технически изисквания за втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток	
REQ.1.	Брой потребители: 500
REQ.2.	Тип решение: Облачно решение за защита за e-mail среда от напреднали атаки за 500 потребителя с включена поддръжка до 14.04.2028г.
REQ.3.	Решението трябва да разполага с функция за анализ както на входящи електронни съобщения (Inbound), така и на изходящи (Outbound), минимално за индивидуални съобщения.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток	
REQ.4.	Решението трябва да разполага с антивирусен метод за откриване и блокиране на заплахи в електронна поща на базата на дефиниции.
REQ.5.	Решението трябва да разполага с механизъм за филтриране на входящи електронни съобщения класифицирани като спам или засечени като част от спам кампания.
REQ.6.	Решението трябва да разполага с функция за засичане и филтриране на входящи съобщения от новосъздадени домейни (например създадени в последните 24 часа).
REQ.7.	Решението трябва да разполага с функция за филтриране на входящи съобщения на базата на черни списъци за IP репутация (RBL).
REQ.8.	Решението трябва да може да засича и филтрира съобщения, които са от тип новинарски (newsletters).
REQ.9.	Решението трябва да разполага с функция за SPF/DKIM/DMARC валидация на входящи съобщения.
REQ.10.	Решението трябва да може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като трябва да се използват технологии и методи за засичане, които да не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а да може да извършва и динамичен анализ и да открива непознати "zero-day" заплахи.
REQ.11.	Решението трябва да се предоставя под формата на облачно решение, като производителят трябва да предостави лицензи за софтуер за виртуални машини за анализ, с прилежащите им операционни системи и приложения.
REQ.12.	Решението трябва да може да открива фишинг и spear-фишинг атаки. Трябва да може да анализира прикачени файлове и URL адреси в електронните съобщения, за да открива опити за компрометиране на системите на организацията.
REQ.13.	Решението трябва да може да открива impersonation атаки (представяне с чужда самоличност). Трябва да се позволява конфигурирането на отношения между имена и email адреси, така че да се засичат опити за impersonation атаки, които копират имената или email адресите на потребителите.
REQ.14.	Решението трябва да може да засича зловреден код с голяма точност, с изключително малък процент на грешни показания. Трябва да може да се открива с точност зловреден код, независимо от MIME тип, тип на разширение (extension) и независимо дали са използвани техники за скриване или архивиране на съдържанието на електронните съобщения.
REQ.15.	Решението трябва да може да поставя в карантина email съобщения, които съдържат URL адреси в тялото си, съдържат MS Office документи, PDF документи, архиви и HTML файлове, замаскирани JAVA скриптове, замаскирани, съкратени или пренасочващи URL адреси.
REQ.16.	Решението трябва да може да анализира множество типове файлове, използвайки различни приложения и техни версии за анализа, съответно за разширения (минимално): exe, dll, pdf, pub, doc, docx, xls, xlsx, js, gif, jpeg, png, tiff, swf, eml, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp.
REQ.17.	Решението трябва да може да извлича и анализира вмъкнати файлове в

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток	
	документи, като например pdf, rtf или MS Office документи.
REQ.18.	Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.
REQ.19.	Решението трябва да може да поставя в карантина и да алармира за прикачени MS Office документи, които съдържат макроси или имат вградени в тях документи, независимо от резултата от анализа.
REQ.20.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.
REQ.21.	За електронни съобщения, които съдържат URL адреси, които водят до сваляне на файлове, решението трябва да може да извлича и анализира въпросните файлове от URL адресите, като да може да се блокира съобщението ако файловете се окажат зловредни.
REQ.22.	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат прикачени JAR файлове или съдържат URL адреси, които водят до JAR файлове.
REQ.23.	Решението трябва да може да извлича и анализира URL адреси от съдържанието на електронните съобщения и от секцията „Относно“ на съобщенията, както и от прикачени PDF или MS Office документи.
REQ.24.	Решението трябва да може да засича следните техники, които се използват от атакуващите хакери, за да подмамят потребителите да достъпят конкретни URL адреси: заместване на знак от адреса с друг (typosquatting), използване на линк към различен адрес от изобразения (URL overlay).
REQ.25.	Решението трябва да може да анализира URL адреси от тип ftp, http и https.
REQ.26.	Решението трябва да може да анализира base64 кодирани URL адреси.
REQ.27.	Решението трябва да анализира прикачени архиви тип 7Z, ZIP, LZH, RAR.
REQ.28.	Решението трябва да може да анализира файлове не само чрез статичен анализ с дефиниции, но и чрез алгоритми за машинно обучение и динамичен анализ тип sandbox.
REQ.29.	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) сваленитe файлове от заявки, идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението трябва да може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази.
REQ.30.	Решението трябва да може да открива с много висока точност, с възможно най-малко грешни показания, файлове, които след анализ на поведението се държат по подобие на зловреден код: поведение, което опитва да избегне засичане, инсталиране на нежелани програми, промени по системните настройки, намаляване на цялостната производителност на системата, потенциално нежелани програми (PUP), потенциално нежелани приложения (PUA), adware процеси, инструменти, които често се използват от атакуващи хакери.
REQ.31.	По време на анализа във виртуалните машини, решението трябва да може да извлича и анализира URL адресите в паметта на машините.
REQ.32.	Решението трябва да може да засича ransomware криптиращи атаки и атаки,

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток	
	предназначени за POS терминали.
REQ.33.	Решението трябва да може да алармира за зловредни процеси (файлове и URL адреси), които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.34.	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на свалените файлове, цялостен одит на действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и да се предоставя информация за хронологчния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.
REQ.35.	Решението трябва да предоставя следствена информация след динамичния анализ на файлове, представена в графичен вид, изобразявайки процеси, достъпи до паметта, промени по файлове и регистри, качени DLL библиотеки, инжектиране на код, heap spraying процеси, mutex процеси.
REQ.36.	Решението трябва да може да предоставя, където е възможно, информация за атакуващата хакерска групировка и възможни стъпки за отстраняване на щетите (remediation) след дадена атака.
REQ.37.	Ако при анализ на зловреден прикачен файл се установят опити за мрежови свързвания извън организацията от него, решението трябва да сигнализира и за тях при вдигането на съответната аларма.
REQ.38.	Решението трябва да може да предоставя screenshot на зареден в браузър зловреден URL адрес по време на анализа му, за да се добие визуална представа за съдържанието на URL адреса.
REQ.39.	Решението трябва да може да прави корелация на електронни съобщения със сходни характеристики, като например с еднакви прикачени файлове, еднакви заглавни части, еднакви изпращачи и т.н. и да може да ги групира като email кампании.
REQ.40.	Решението трябва да може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.
REQ.41.	Решението не трябва да използва комерсиален хипервайзор за анализ, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н. Решението трябва да използва собствен, специално изграден хипервайзор.
REQ.42.	Решението трябва да може да засича опити за използване на функциите за приспиване (sleep) на операционните системи от зловредния код и да може да забързва времето на виртуалните машини за анализ, за да принуди изпълнението на зловредния код.
REQ.43.	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток	
REQ.44.	Решението трябва да поддържа inline режим на работа за блокиране на зловредни входящи съобщения.
REQ.45.	Решението трябва да поддържа BCC/OOB режим на работа.
REQ.46.	Решението трябва да позволява (по избор от администратор) извършване на динамичен анализ на файлове във виртуалните машини, както в режим на изолация (без да е необходима свързаност с Интернет), така и с позволено мрежово свързване от виртуалните машини („жив“ режим), за да се добие цялостен анализ на зловредния код.
REQ.47.	Решението трябва да използва специално заделен мрежови интерфейс, когато е пуснато в „жив“ режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; мрежовият интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни артефакти, които са му необходими, за да се изпълни изцяло анализа.
REQ.48.	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код, изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.
REQ.49.	Цялостният анализ на електронното съобщение не трябва да отнема повече от 10 минути.
REQ.50.	Решението трябва да позволява използването на YARA правила и да позволява конфигурирането на автоматични аларми или поставяне в карантина, ако дадено съобщение отговаря на зададените YARA правила.
REQ.51.	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.
REQ.52.	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.
REQ.53.	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.
REQ.54.	Решението трябва да може да изпраща автоматични известия, когато блокира или постави в карантина дадено електронно email съобщение.
REQ.55.	Решението трябва да позволява администрация чрез уеб-базирана облачна конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.56.	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.), като да задават кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.57.	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.
REQ.58.	Решението трябва да позволява групирането на аларми за зловредни email съобщения по поне следните критерии: по изпращачи, по получатели, по видове вдигнати аларми, по email кампания.
REQ.59.	Решението трябва да позволява генерирането на отчети в PDF или в CSV формат, според типа информация в тях: вдигнати аларми и техните детайли,

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за втори слой сензор за анализ на киберзаплахи, свързани с проверка на зловредни файлове и phishing връзки в имейл поток	
	тип инфекция, обобщителна информация за предоставяне пред ръководните органи на организацията, списък с достъпените сървъри при callback комуникация и други.
REQ.60.	Решението трябва да позволява извличането на метаданни от email съобщенията, минимално получател, прикачени файлове и вмъкнати URL адреси, като тези метаданни да могат да се изпращат към решение тип SIEM, чрез HTTP или чрез Rsyslog протокол.
Гаранция и поддръжка:	
REQ.61.	Срок: до 14.04.2028г.
REQ.62.	Тип поддръжка: 24x7x365
REQ.63.	Възможност за актуализиране на софтуера в периода на поддръжката до последна актуална версия на производителя.

4. **Платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни, придобити от платформа за мониторинг на киберзаплахи и Darkweb**

Минимални технически изисквания за платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни придобити от платформа за мониторинг на киберзаплахи и Darkweb	
REQ.1.	Предложеното решение трябва да включва лицензи за събиране на до 50GB данни за събития на ден, с валидност и включена поддръжка до 14.04.2028г. разширени лицензи за съхранение на събраните данни за период минимално от 180 календарни дни, с валидност и включена поддръжка до 14.04.2028г.; лицензи за добавяне на функции чрез корелация на данни и събития.
REQ.2.	Решението трябва да разполага с централизирана конзола за управление под формата на SaaS. Достъпът до конзолата трябва да може да се предоставя през уеб-базиран потребителски интерфейс, както и чрез REST API интерфейс.
REQ.3.	Всички компоненти на решението трябва да са предоставени от единен производител. Не се разрешава използването на множество решения от различни производители.
REQ.4.	Платформата на решението трябва да е в съответствие с изискванията на стандартите за киберсигурност ISO/IEC 27001:2022 и SOC 2 Type 2.
REQ.5.	Платформата на решението трябва да разполага със следните защитни механизми: -многофакторна автентикация чрез TOTP токени -възможност за интеграция с външно решение за управление на идентичности чрез SAML 2.0 -автоматично отписване на акаунт след предварително зададен период на неактивност на потребителите -ролево-базиран контрол на достъпа

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни придобити от платформа за мониторинг на киберзаплахи и Darkweb	
REQ.6.	Решението трябва да позволява да се конфигурира грануларен достъп на достъпващите го потребители, минимално: -цялостен достъп до платформата -достъп само до определени модули на платформата -достъп само за четене на информация от платформата
REQ.7.	Платформата на решението трябва да може да предоставя от единна конзола достъп до всички необходими модули за ефективна киберсигурност икорелационни функционалности, както за данни, директно събрани от платформата за мониторинг за киберзаплахи, така и от трети източници.
REQ.8.	Платформата трябва да разполага със специално изградена за облак архитектура (cloud-native), а да не е пригодена за облак чрез „lift-and-shift“ процес.
REQ.9.	Платформата трябва да разполага с модерна архитектура и високо ниво на компресиране на събраните данни, така че да може да работи с петабайти от данни, предоставяйки функции за бързо търсене в тях.
REQ.10.	Платформата трябва да разполага с единен езиков модел за изготвяне на заявки за търсене на информация измежду всичките ѝ компоненти, така че да се улесни работата на анализаторите.
REQ.11.	Платформата трябва да разполага с multi-tenancy модел на работа, за сложни и географски разпръснати организации.
REQ.12.	Платформата трябва да е изградена за разширяване на функциите за разследване върху събраните данни от крайни точки от решенията за защита и разследване на заплахи на крайни точки от същия производител, с възможност за добавяне на информация от трети източници за цялостна видимост над възникналите събития в организацията.
REQ.13.	Платформата трябва да разполага с множество конектори по подразбиране за събиране на данни от различни източници.
REQ.14.	Платформата трябва да разполага с множество парсери на данни, които да са лесни за имплементиране.
REQ.15.	Платформата трябва да позволява използването на HTTP колектор на събития (HEC) за лесна интеграция на трети източници.
REQ.16.	Платформата трябва да разполага с помощник в изграждането на заявки за търсене на информация под формата на изкуствен интелект/машинно-самообучение, като генерираните заявки трябва да могат да се модифицират.
REQ.17.	Платформата трябва да позволява да се мониторират всички процеси по събиране на логове, както и да може да се следи работното състояние на тези процеси.

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни придобити от платформа за мониторинг на киберзаплахи и Darkweb	
REQ.18.	Платформата трябва да разполага с добре описан API интерфейс за интеграция с трети решения.
REQ.19.	Платформата трябва да поддържа използването на модели за по-ефективно придвижване на различни типове данни към нея. Трябва да се поддържат минимално модели за придвижване на структурирани данни, неструктурирани данни, сурови данни, телеметрични данни.
REQ.20.	Платформата трябва да позволява добиването на данни, без да е необходимо те да са предварително индексирани.
REQ.21.	Платформата трябва да позволява да могат да се нормализират данни от различни информационни полета и формати на данни за целите на ускорен анализ.
REQ.22.	Платформата трябва да позволява + и интеграция по подразбиране на различни компоненти от екосистемата за киберсигурност на производителя, с цел потенциално бъдещо надграждане с решения като: -разширени функции за анализ и ответни мерки на инциденти (XDR) -разширени функции за анализ и ответни мерки на инциденти на ниво крайна точка (EDR) -информация за възникнали и потенциални заплахи (Threat intelligence) -платформа за защита на облачни приложения (CNAPP) -решение за засичане на заплахи и ответни мерки на инциденти, свързани с идентичности (ITDR) -антивирус от ново поколение (NGAV) -защита на данни
REQ.23.	Платформата трябва да поддържа минимално следните нива на критичност на възникналите аларми: информационни, ниско, средно, високо или критично ниво.
REQ.24.	Платформата трябва да може да работи без внесено забавяне в процесите по събиране и обработване на логове, да алармира за заплахи и да предоставя данни, в които да може да се търси в реално време.
REQ.25.	Платформата трябва да може автоматично да групира сходни аларми за по-бързо и лесно триажиране на информация и анализ на инциденти.
REQ.26.	Платформата трябва да позволява управлението на инциденти с минимално следните функции: 1. Да може да се обвърже даден инцидент с конкретен анализатор 2. Да може да се поставя и променя статус на даден инцидент: * Нов

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни придобити от платформа за мониторинг на киберзаплахи и Darkweb	
	* В момента обработван * Отворен повторно * Затворен 3. Да могат да се добавят бележки към засечените инциденти 4. Да могат да се поставят тагове на засечените инциденти
REQ.27.	Платформата трябва да може да обвързва засечените заплахи с MITRE ATT&CK рамковия модел за киберсигурност.
REQ.28.	Платформата трябва да позволява достъпването и прегледа на данни в исторически план, за целите на извършване на разследване в големи обеми от събрани данни.
REQ.29.	Платформата трябва да позволява изграждането на собствени табла/конзоли за информация в интерфейса на решението, използвайки предефинирани контроли или изградени контроли на базата на направени заявки за търсене в събраните телеметрични данни.
REQ.30.	Платформата трябва да позволява търсене из всички събрани телеметрични данни чрез помощници или чрез писането ръчно на заявки за търсене на информация. Заявките трябва да позволяват комбинирането на различни телеметрични данни от различни източници, като да могат да се филтрират и да могат да се трансформират крайните резултати от тях. Правилата за изграждане на заявки трябва да са добре описани в документацията на решението.
REQ.31.	Платформата трябва да позволява запазването на направени заявки за търсене на информация в телеметрични данни в глобално достъпна библиотека на решението.
REQ.32.	Платформата трябва да позволява изпълнението на заявки за търсене на информация в телеметрични данни и изобразяването на резултатите от тях чрез API.
REQ.33.	Платформата трябва да позволява извличането на резултати от заявки за търсения на информация в минимално следните формати: CSV, JSON, NDJSON, текстови формат.
REQ.34.	Платформата трябва да позволява автоматичното извършване на заявки за търсене на информация на цикличен принцип по предварително зададен график или еднократно в предварително зададено време, като резултатите да могат да се изпращат автоматично към посочени email адреси.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни придобити от платформа за мониторинг на киберзаплахи и Darkweb	
REQ.35.	Платформата трябва да разполага с логични правила за корелации по подразбиране, които да могат да се тестват периодично и да могат да се модифицират при необходимост.
REQ.36.	Платформата трябва да позволява преобразуването на заявка за търсене на информация в събраните телеметрични данни в правило за корелация на информация, което да може да се изпълнява по предварително зададен график, генерирайки аларми, ако заявката върне повече от един запис.
REQ.37.	Платформата трябва да разполага с минимално следните функции за обработане на логове от трети системи: * Съхранение на събраните логове за минимум 7 дни * Поддръжка на минимално следните системи за събиране на логове: 1. Palo Alto Networks защитни стени 2. Fortinet защитни стени 3. Proofpoint Email Security 4. Cisco Secure Email Gateway 5. VMware ESXi 6. Microsoft Azure Event хъбове 7. Microsoft Exchange Online 8. Microsoft Graph API 9. Vectra AI 10. ZScaler 11. Универсален HTTP колектор на събития
REQ.38.	Платформата трябва да разполага с функции за управление на инциденти, които да позволяват създаването на доклад за инцидент при засичане на заплаха или група от свързани заплахи, за да може да се изобразява и съхранява информацията за заплахите в организиран вид.
REQ.39.	Платформата трябва да разполага с напреднали функции за визуализация на данните от дадено разследване, като графики с взаимовръзките на замесените активи в даден инцидент, графики с пътя на дадена атака и времедиаграми на възникналите събития за пълна видимост над възникналите инциденти в удобен формат.
REQ.40.	Платформата трябва да предоставя функции в реално време за колаборация между множество анализатори, позволявайки им да си споделят данни и да документират заедно през платформата откритите инциденти.

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Минимални технически изисквания за платформа за събиране и корелация на данни, придобити от сензори за анализ на мейл поток и данни придобити от платформа за мониторинг на киберзаплахи и Darkweb	
REQ.41.	Решението трябва да разполага с функции за одит на действията с платформата му, запазвайки всички действия в лог файл, придружени с данни за време на настъпване, информация кой потребител е извършил действието и използван метод.
Гаранция и поддръжка:	
REQ.42.	Срок: до 14.04.2028г.
REQ.43.	Тип поддръжка: 24x7x365
REQ.44.	Възможност за обновление на софтуера в периода на поддръжката
REQ.45.	Възможност за обновления на информацията за заплахите от базата данни на производителя

III. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

В случай че не е производител, участникът в обществената поръчка следва да е надлежно оторизиран от производителя на софтуерните продукти или официален негов представител за правото на разпространение/доставка на предлаганите софтуерни продукти.

IV. СРОК НА ИЗПЪЛНЕНИЕ. УСЛОВИЯ НА ДОСТАВКА

Срокът за доставка на платформата е до 30 (тридесет) работни дни от датата на подписване на договор с избран изпълнител по ЗОП.

Срокът на гаранционна поддръжка е съобразно предложения от избрания изпълнител в офертата му срок, считано от датата на приемо-предавателния протокол за осигуряване на решенията или от датата на регистрация в портала на производителя, което обстоятелство настъпи първо.

V. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

Мястото на осигуряване на решенията и услугите по техническата поддръжка, при необходимост от оказване на съдействие на място, е сградата на Министерство на здравеопазването, с адрес: гр. София, пл. “Света Неделя” № 5.

Услугите по гаранционна поддръжка се предоставят отдалечено.

VI. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[2]

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/МЗ/Изпълнителя и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

a. Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Възложителя/МЗ ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.
b. При предоставяне на Услугата спазва правилата за сигурността на информацията на Възложителя/МЗ. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на Възложителя/МЗ, подписват декларации по образец на Възложителя за опазване на информацията, които се предават на Възложителя. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до 2 (два) работни дни от промяната.
c. определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Възложителя при възникване на инцидент по МИС;
d. осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения 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.

3. Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Възложителя/ МЗ.
4. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

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

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

a. При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на Възложителя/МЗ;
b. Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);
c. При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Възложителя/МЗ;
d. 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 Възложителя/МЗ, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на МЗ от страна на Възложителя и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.

Приложение №2

към Договор № ……

(Образец)

Д Е К Л А Р А Ц И Я

ЗА ОПАЗВАНЕ НА ИНФОРМАЦИЯ

Долуподписаният/ та ……..,

ЕГН: .....,[3] в качеството ми на ……., декларирам, че ще пазя в тайна, станалата ми известна във връзка с изпълнението на Договор № ……/…..... г.[4] информация, съдържаща данни, представляващи данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация. За неизпълнение на тези задължения ми е известно, че нося предвидената в съответните нормативни актове отговорност.

Запознат/а съм с разпоредбата на чл. 270 от *Данъчно-осигурителния процесуален кодекс*, съгласно която, ако разглася, предоставя, публикувам, използвам или разпространя по друг начин факти и обстоятелства, представляващи

[3] *В случай, че лицето е чужденец, се вписват съответните идентификационни данни.*

[4] *Вписва се референтен номер на Договора, в договорния регистър на ВЪЗЛОЖИТЕЛЯ.*

"Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация" 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.

данъчна и осигурителна информация, ако не подлежа на по-тежко наказание, ще бъда наказан/а с глоба от 1000 лв. до 5000 лв., а в особено тежки случаи - от 5000 лв. до 10 000 лв.

Декларирам, че ще пазя в тайна, станалата ми известна информация, относно съдържанието на документация, вътрешни правила, процедури, организация, структура, начин на функциониране, комуникации, мрежи и информационни системи на Министерство на електронното управление (ВЪЗЛОЖИТЕЛЯ) и на Министерство на здравеопазването (БЕНЕФИЦИЕРА), изготвени в хода на изпълнението документи и/или всякакви други постигнати резултати от изпълнението, както и че няма да разгласявам, използвам или предоставям на трети лица разработена в полза на БЕНЕФИЦИЕРА документация или програмен код в явен и изпълним вид във връзка с изпълнението на този договор, с изключение на случаите, когато съм задължен по закон за това.

При обработването на данните се задължавам да спазвам разпоредбите на *Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО* и *Закона за защита на личните данни*.

Известна ми е отговорността по чл. 284 от *Наказателния кодекс*, а именно: налагане на наказание лишаване от свобода до две години или пробация, ако във вреда на държавата, на предприятие, организация или на частно лице съобщя другиму или обнародвам информация, която ми е поверена или достъпна по служба и за която зная, че представлява служебна тайна.

Ще спазвам изискванията на действащата нормативна уредба в областта на мрежовата и информационната сигурност.

Известна ми е отговорността по Глава 9а от Особената част на *Наказателния кодекс*, относно достъп до компютърни данни в компютърна система без разрешение, добавяне, промяна, изтриване или унищожаване на компютърна програма или компютърни данни, въвеждане на компютърен вирус в компютърните системи или мрежи на БЕНЕФИЦИЕРА, разпространение на пароли или кодове за достъп до компютърна система или до компютърни данни и от това последва разкриване на лични данни или информация, представляваща държавна или друга защитена от закон тайна.

Подпис:

(подписване с електронен подпис)

“Този документ е създаден с финансовата подкрепа на програма „Научни изследвания, иновации и дигитализация за интелигентна трансформация“ 2021-2027, съфинансирана от Европейския съюз чрез Европейския фонд за регионално развитие.