ИНФОРМАЦИОННО ОБСЛУЖВАНЕ
1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, ЕИК: 831641791
office@is-bg.net www.is-bg.net

ПОКАНА

„Информационно обслужване" АД, със седалище и адрес на управление: гр. София, ул. „Панайот Волов" № 2, тел. 02/9420340, e-mail: office@is-bg.net, представлявано от **Ивайло Филипов – Изпълнителен директор**, Ви кани да участвате в процедура за избор на доставчик, при следните условия:

1. **Предмет на процедурата:**

„Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване" АД".

Количествената и техническа спецификация за доставка на решение за виртуализация на дискови масиви за нуждите на „Информационно обслужване" АД е посочена в Техническо задание – Приложение №1.

2. **Място на доставка и срок за изпълнение:**

2.1. Място на доставка – гр. София, ул. „Лъчезар Станчев" № 20.

2.2. Срок за доставка на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване" АД" – до 10 работни дни, считано от датата на сключване на договор.

2.3. Срок на лицензите – 60 месеца, считано от датата на приемо-предавателния протокол за доставка.

3. **Критерии за оценка на предложенията:** „най-ниска предложена цена".

Участниците се класират според предложената от тях обща цена в лева без ДДС. На първо място се класира участникът, предложил най-ниска цена. Оценката на предложенията се извършва съгласно Методика за оценка на предложенията, приложена към настоящата покана (Приложение № 2).

4. **Списък на документите, които кандидатите следва да представят:**

4.1. Документи за идентификация и квалификация:

4.1.1. Оторизационно писмо или друг еквивалентен документ, издаден от производителя или от официален негов представител на български език или придружени от превод на български език.

В случаите на представяне от Участника на оторизационно писмо от официален представител на производителя (или еквивалентен документ), в предложението се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя, на български език или придружен от превод на български език.

4.1.2. Декларация по образец – Приложение № 5.

4.2. Техническо предложение, изготвено по образец - Приложение № 3.

4.3. Ценово предложение, изготвено по образец - Приложение № 4.

5. Начин на плащане: извършва се по банков път, на 5 равни годишни вноски. Първата годишна вноска се плаща в срок до 30 (тридесет) дни след подписване на приемо-предавателен протокол, удостоверяващ извършването на доставката без възражения и забележки от страна на Възложителя и издадена фактура от Изпълнителя. Следващите 4 годишни вноски се плащат в срок до 30 (тридесет) дни след издадена в началото на всеки период фактура от Изпълнителя.

Максимална обща цена – кандидатите следва да предложат цена, която не надвишава определената максимална обща цена от 670 700 (шестстотин и седемдесет хиляди и седемстотин) лв. без ДДС.

Кандидат, предложил по-висока от максималната обща цена, ще бъде отстранен от участие в процедурата.

7. Срок на валидност на предложението - срокът на валидност да бъде не по-малко от 60 (шестдесет) календарни дни, считано от датата на представяне на предложението.

8. Подаване на предложението:

8.1. Срок, място и начин:

Предложението следва да бъде подадено по електронен път в срок **до 12:00 часа на 23.12.2025г.**, на следния адрес на електронна поща: office@is-bg.net.

8.2. Изисквания към подаване на предложението:

Техническото предложение (Приложение № 3), Ценовото предложение (Приложение № 4) и Декларацията (Приложение № 5) се съставят като електронни документи във формат .pdf и се подписват с квалифициран електронен подпис.

Ако към предложението е необходимо да бъде представен документ, който е издаден на хартиен носител, същият се представя сканиран и заверен с квалифициран електронен подпис.

В случай, че обстоятелства от документите за идентификация и квалификация са достъпни чрез публичен безплатен регистър или информацията е публично достъпна на друг официален адрес, кандидатите могат да посочат електронен адрес, на който тази информация е налична и достъпна.

Електронното съобщение, с което се подава предложението в настоящата процедура, следва да съдържа данни за:

1. наименованието на участника;
2. телефон и електронен адрес;
3. наименованието на процедурата, за която се подават документите.

За дата и час на получаване на предложението се приемат датата и часа на получаване на предложението на посочения в т. 8.1 адрес на електронна поща за подаване на предложения.

„Информационно обслужване“ АД използва инструменти за гарантиране на сигурността на информацията, предавана по електронна поща, които могат да забавят получаването на електронни съобщения, поради което е препоръчително предложенията в настоящата процедура да се изпращат най-малко 30 минути преди крайния срок по т. 8.1.

9. Лице за контакти с „Информационно обслужване” АД

Юлиян Димитров, заместник ръководител, отдел „Киберзащита и управление на информационната сигурност“, мобилен: +359 876 869 714, e-mail: y.p.dimitrov@is-bg.net.

10. Участници в процедурата

В процедурата могат да участват и кандидати, до които не е изпратена изрична покана.

Приложения:

Техническо задание – Приложение № 1;
Методика за оценка на предложенията – Приложение № 2;
Техническо предложение – образец - Приложение № 3;
Ценово предложение – образец - Приложение № 4;
Декларация – образец – Приложение № 5;
Указания за участие в процедурата – Приложение № 6.

ИВАЙЛО ФИЛИПОВ
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ” АД

Приложение № 1

ТЕХНИЧЕСКО ЗАДАНИЕ

с

Количествена и техническа спецификация

за придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД.

Предложеното решение трябва да включва инсталация на **1 400 агента** и да отговаря на следните минимални технически параметри:

Параметър
Участникът трябва да достави всички необходими лицензи с права за ползване на всички изисквани функционалности за защита на **1350** работни станции и сървъри и за сигурност на облачни среди (CNAPP) за **50** крайни точки, което да включва Cloud Runtime Security (с CDR, CWP и WAAS), CSPM, CIEM, DSPM. за период от 60 (шестдесет) месеца.
Антивирусни функционалности от следващо поколение базирани на машинно обучение, локален анализ и предотвратяване на заплахи
Предотвратяване на заплахи, базирано на поведение и динамичен анализ на работещи процеси
Предотвратяване на експлоатация чрез техника на експлоатиране
Автоматизирана интеграция с базирана в облак услуга за предотвратяване на злонамерен софтуер, с отчети за анализ и поддръжка на минимум 100MB размера на файла
Модул за инспекция на мрежата с цел спиране на мрежови атаки в случай че бъде направена интеграция с устройства за мрежова сигурност
Възможност за създаване на профили за сигурност и задаване на изключения
Извънредно и планирано сканиране на крайни точки
Защита срещу злонамерен софтуер, крипто вируси и атаки без файлове
Унифициран олекотен агент за защита, откриване и реакция срещу заплахи на крайните точки
Защитна стена на хоста
Криптиране на диска
Управление на USB устройства
Персонализирани правила за превенция
Автоматично групиране на свързани сигнали от различни източници в един инцидент

Интуитивен изглед на инцидента с преглед на инцидента и тактики на MITRE и ключова информация за инцидента.
Възможност за персонализирано оценяване на инциденти
Списък на забележителни артефакти от сигнали и обогатена информация от услуга за разузнаване за заплахи
Изброяване на потребители и хостове, участващи в инциденти, за бързо определяне на обхвата на инцидента
Възможност за възлагане на конкретни инциденти на членовете на екипа
Възможност за добавяне на коментари към инциденти
Обединяване на инциденти по избор
Възможност за отдалечен терминал
Възможност за изпълнение на команди и скриптове на CMD, PowerShell и Python в Windows
Възможност за изпълнение на команди на Bash и Python на macOS и Linux
Отдалечено изолиране на единична крайна точка или множество крайни точки
Отдалечено изтриване на файл на една или няколко крайни точки
Възможност за преглеждане, спиране или прекратяване на работещи процеси или изтегляне на двоични файлове с графичен мениджър на задачи за Windows, macOS и Linux
Мащабируемо, базирано на облак управление, както и инсталиране на агент
Единна уеб-базирана конзола за управление за сигурността на крайните точки, както и разширено откриване и реакция
Контрол на достъпа, базиран на роли (RBAC) за персонализирани права
Възможност за мултифакторна автентикация (MFA)
Персонализирани информационни табла за високо ниво на сигурност и оперативна информация
Инструменти за управление на трети страни базирани на стандарти приложно програмни интерфейси , които се интегрират и извършват административни действия
Решението да включва права за използване на облачна среда за съхранение и анализиране на логове от крайни устройства и защитни стени с капацитет минимум 150GB на ден и 30 дневен период за съхранение.
Решението да предлага възможност за бъдещо надграждане към единна платформа за откриване, управление и автоматизиране на инциденти, като включва минимум SIEM, SOAR, Attack Service Management, Threat Intel Management, UEBA с капацитет минимум 200G на ден и 30 дневен период за запазване на данни.

Агента на решението да може да бъде инсталиран на минимум: ● Windows 10 и по-нови ● Windows Server 2012 и по-нови ● macOS 13 и по-нови ● ORACLE 6 и по-нови ● Debian 9 и по-нови ● RedHat 6 и по-нови ● Ubuntu ● CentOS ● Android ● iOS
Сертификация на производителя по ISO 27001
Автоматизирано свързване на данни от крайни точки, мрежа, облак и данни за самоличност, включително предупреждения и събития за сигурност
Автоматизиран анализ на първопричината за всеки сигнал, включително мрежови сигнали, ако има налични данни за крайната точка
Да има възможност за предоставяне на анализа във времева линия, за да може да се видят всички действия и сигнали и тяхната последователност
Решението да има възможност за 360-градусов изглед към потребителите и съответните оценки на техния риск
Възможност за използване на база за разузнаване (Threat Intelligence) на заплахи от източници на трети страни във формати JSON и CSV
Откриване и отговор на заплахи, включващи управлявани и неуправлявани крайни точки
Откриване и реагиране на заплахи, включващи облачни сървъри
Непрекъснато събиране и централизирано съхранение на всички данни за сигурност с цел поведенчески анализи
Решението да прави анализ на крайните устройства включително инвентаризация, оценка и управление на уязвимости, както и незабавно намиране и премахване на заплахи
Възможност с допълнителен лиценз за запазване на данни за неограничен период от време.
Една година задържане за одитни дневници на административна и следствена дейност
Решението да може да се интегрира с външна система като SLACK и Syslog за изпращане на известия при инцидент.

Решението да покрива минимум 200 броя Windows машини с включена функционалност за събиране, задълбочен анализ и разследване на данни като включва минимум : ● История на браузъра (Chrome, Edge, Firefox, Internet Explorer) ● Достъп до файлове ● Стартиране на процеси ● Мрежова активност ● История на команди ● Отдалечен достъп
Софтуерна гаранционна поддръжка от производителя за 60 месеца.

Приложение № 2

Методика за оценка на предложенията,

подадени в процедура за избор на доставчик с предмет:

„Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“

1. Предложенията се оценяват за съответствие с техническите изисквания в Техническото задание - Приложение № 1.

2. Предложенията, отговарящи на изискванията по т. 1, се оценяват по критерия „най-ниска предложена цена“, като се сравнява предложената обща цена в лева без ДДС.

3. На първо място се класира участникът, предложил най-ниска цена, като участниците се подреждат по възходящ ред.

Приложение № 3

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ“ № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

за

участие в процедура за избор на доставчик с предмет:

„Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“

След запознаване с поканата за участие в процедура за избор на доставчик с предмет: „Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“, с настоящото Техническо предложение правим следните обвързващи предложения:

1. Срок за изпълнение:
   1.1. Декларираме, че ще доставим лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции в срок до ……..…/……/ дни (*не повече от десет работни дни*), считано от датата на сключване на договор.
   1.2. Срокът на лицензите и софтуерната гаранционна поддръжка от производителя е 60 месеца, считано от датата на приемо-предавателния протокол за доставка.
2. Приемаме да изпълним предмета на процедурата, съгласно всички условия и изисквания, посочени от Възложителя в поканата за участие в настоящата процедура и Техническото задание - Приложение № 1.
3. Предложението е със срок на валидност …….. / ……/ календарни дни *(не по-малко от 60 /шестдесет/ календарни дни)*, считано от датата на представяне на предложението.
4. Приемаме да доставим лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции, отговарящо на следните технически параметри:

Параметър
Участникът трябва да достави всички необходими лицензи с права за ползване на всички изисквани функционалности за защита на **1350** работни станции и сървъри и за сигурност на облачни среди (CNAPP) за **50** крайни точки, което да включва Cloud Runtime Security (с CDR, CWP и WAAS), CSPM, CIEM, DSPM. за период от 60 (шестдесет) месеца.
Антивирусни функционалности от следващо поколение базирани на машинно обучение, локален анализ и предотвратяване на заплахи
Предотвратяване на заплахи, базирано на поведение и динамичен анализ на работещи процеси
Предотвратяване на експлоатация чрез техника на експлоатиране
Автоматизирана интеграция с базирана в облак услуга за предотвратяване на злонамерен софтуер, с отчети за анализ и поддръжка на минимум 100MB размера на файла
Модул за инспекция на мрежата с цел спиране на мрежови атаки в случай че бъде направена интеграция с устройства за мрежова сигурност
Възможност за създаване на профили за сигурност и задаване на изключения
Извънредно и планирано сканиране на крайни точки
Защита срещу злонамерен софтуер, крипто вируси и атаки без файлове
Унифициран олекотен агент за защита, откриване и реакция срещу заплахи на крайните точки
Защитна стена на хоста
Криптиране на диска
Управление на USB устройства
Персонализирани правила за превенция
Автоматично групиране на свързани сигнали от различни източници в един инцидент
Интуитивен изглед на инцидента с преглед на инцидента и тактики на MITRE и ключова информация за инцидента.
Възможност за персонализирано оценяване на инциденти
Списък на забележителни артефакти от сигнали и обогатена информация от услуга за разузнаване за заплахи
Изброяване на потребители и хостове, участващи в инциденти, за бързо определяне на обхвата на инцидента
Възможност за възлагане на конкретни инциденти на членовете на екипа
Възможност за добавяне на коментари към инциденти
Обединяване на инциденти по избор

Възможност за отдалечен терминал
Възможност за изпълнение на команди и скриптове на CMD, PowerShell и Python в Windows
Възможност за изпълнение на команди на Bash и Python на macOS и Linux
Отдалечено изолиране на единична крайна точка или множество крайни точки
Отдалечено изтриване на файл на една или няколко крайни точки
Възможност за преглеждане, спиране или прекратяване на работещи процеси или изтегляне на двоични файлове с графичен мениджър на задачи за Windows, macOS и Linux
Мащабируемо, базирано на облак управление, както и инсталиране на агент
Единна уеб-базирана конзола за управление за сигурността на крайните точки, както и разширено откриване и реакция
Контрол на достъпа, базиран на роли (RBAC) за персонализирани права
Възможност за мултифакторна автентикация (MFA)
Персонализирани информационни табла за високо ниво на сигурност и оперативна информация
Инструменти за управление на трети страни базирани на стандарти приложно програмни интерфейси , които се интегрират и извършват административни действия
Решението да включва права за използване на облачна среда за съхранение и анализиране на логове от крайни устройства и защитни стени с капацитет минимум 150GB на ден и 30 дневен период за съхранение.
Решението да предлага възможност за бъдещо надграждане към единна платформа за откриване, управление и автоматизиране на инциденти, като включва минимум SIEM, SOAR, Attack Service Management, Threat Intel Management, UEBA с капацитет минимум 200G на ден и 30 дневен период за запазване на данни.
Агента на решението да може да бъде инсталиран на минимум: ● Windows 10 и по-нови ● Windows Server 2012 и по-нови ● macOS 13 и по-нови ● ORACLE 6 и по-нови ● Debian 9 и по-нови ● RedHat 6 и по-нови ● Ubuntu ● CentOS ● Android ● iOS
Сертификация на производителя по ISO 27001
Автоматизирано свързване на данни от крайни точки, мрежа, облак и данни за самоличност, включително предупреждения и събития за сигурност
Автоматизиран анализ на първопричината за всеки сигнал, включително мрежови сигнали, ако има налични данни за крайната точка

Да има възможност за предоставяне на анализа във времева линия, за да може да се видят всички действия и сигнали и тяхната последователност
Решението да има възможност за 360-градусов изглед към потребителите и съответните оценки на техния риск
Възможност за използване на база за разузнаване (Threat Intelligence) на заплахи от източници на трети страни във формати JSON и CSV
Откриване и отговор на заплахи, включващи управлявани и неуправлявани крайни точки
Откриване и реагиране на заплахи, включващи облачни сървъри
Непрекъснато събиране и централизирано съхранение на всички данни за сигурност с цел поведенчески анализи
Решението да прави анализ на крайните устройства включително инвентаризация, оценка и управление на уязвимости, както и незабавно намиране и премахване на заплахи
Възможност с допълнителен лиценз за запазване на данни за неограничен период от време.
Една година задържане за одитни дневници на административна и следствена дейност
Решението да може да се интегрира с външна система като SLACK и Syslog за изпращане на известия при инцидент.
Решението да покрива минимум 200 броя Windows машини с включена функционалност за събиране, задълбочен анализ и разследване на данни като включва минимум : ● История на браузъра (Chrome, Edge, Firefox, Internet Explorer) ● Достъп до файлове ● Стартиране на процеси ● Мрежова активност ● История на команди ● Отдалечен достъп
Софтуерна гаранционна поддръжка от производителя за 60 месеца.

ПОДПИС

[име и фамилия]

[качество на представляващия участника]

Забележка: *Техническото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 4

Образец

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

УЛ. „ПАНАЙОТ ВОЛОВ” № 2

ГР. СОФИЯ

[наименование на участника],
представлявано от [трите имена] в качеството на [длъжност, или друго качество]
с ЕИК […], със седалище […] и адрес на управление […],
адрес за кореспонденция: […],
банкови сметки: […]

ЦЕНОВО ПРЕДЛОЖЕНИЕ

за

участие в процедура за избор на доставчик с предмет:

„Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“

След запознаване с поканата за участие в процедура за избор на доставчик с предмет: „**Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“** и Техническото задание на Възложителя, ние представяме следното Ценово предложение:

1. Предлагаме да доставим **лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции**, предмет на горецитираната процедура, в съответствие с Техническото задание на Възложителя – Приложение № 1 и представеното от нас Техническо предложение – Приложение № 3 **при обща цена в размер ……..…….. (словом: ……..) лева без ДДС.**

2. Декларираме, че в предложената цена са включени всички разходи за изпълнение на дейностите, предмет на процедурата, включени в Техническото задание на Възложителя и представеното от нас Техническо предложение.

3. Начин на плащане – извършва се по банков път, на 5 равни годишни вноски. Първата вноска се плаща в срок до ……../не по-малко от 30 дни/ след подписване на приемо-предавателен протокол, удостоверяващ извършването на доставката без възражения и забележки от страна на

Възложителя и издадена фактура от Изпълнителя. Следващите 4 годишни вноски се плащат в срок до 30 (тридесет) дни след издадена в началото на всеки период фактура от Изпълнителя.

[дата]

ПОДПИС
[име и фамилия]
[качество на представляващия участника]

Забележка: *Ценовото предложение се представя в електронен вид във формат .pdf, подписано с квалифициран електронен подпис.*

Приложение № 5

Образец

ДЕКЛАРАЦИЯ

От.....,

представляващ ..... – кандидат в процедура с предмет: „**Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“**, в качеството ми на .....,

ДЕКЛАРИРАМ, че представляваното от мен дружество:

1. Не е обявено в несъстоятелност и не е в производство за обявяване в несъстоятелност;
2. Не е в производство по ликвидация.

ДЕКЛАРИРАМ, че:

3. Не съм лишен от правото да упражнявам търговска дейност;
4. Не съм осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, включително изпиране на пари, по чл. 253 – 260 от НК, за подкуп по чл. 301 – 307 от НК, участие в организирана престъпна група по чл. 321 и чл. 321а от НК, както и за престъпление против собствеността по чл. 194 – 217 от НК или против стопанството по чл. 219 – 252 от НК.

ДЕКЛАРАТОР:

Забележки:

1. Декларацията се представя в електронен вид във формат .pdf, подписана с квалифициран електронен подпис.

2. Декларацията се подписва задължително от управляващия и представляващ дружеството. Когато управляващите дружеството са повече от едно лице, декларацията се подписва от всички лица, вписани в Търговския регистър като представляващи и се представя в отделен екземпляр за всяко представляващо лице.

Приложение № 6

УКАЗАНИЯ

за участие в процедура за избор на доставчик с предмет:

„Придобиване на лицензи за решение за разширено откриване и реагиране на заплахи на крайни работни станции за период от 60 месеца за нуждите на „Информационно обслужване“ АД“

1. Кандидатите изготвят и окомплектоват предложенията си съгласно изискванията, посочени в поканата и приложенията към нея.
2. Не по-късно от 11:00 ч. на 22.12.2025 г. всеки кандидат може да поиска от Възложителя писмено разяснения по документацията. Възложителят изпраща разяснението до всички кандидати, които са получили документация за участие и са посочили адрес за кореспонденция и го публикува на интернет-страницата на „Информационно обслужване” АД.
3. Предложенията се приемат по начина и в срока, посочени в поканата. Приемат се и предложения на кандидати, които не са поканени с изрична покана.
4. Предложение, получено след изтичане на крайния срок, не се разглежда от Възложителя. В този случай до кандидата се изпраща уведомление.
5. Изборът на доставчици се извършва въз основа на подадените предложения.
6. Изпълнителният директор на „Информационно обслужване” АД назначава комисия за разглеждането и оценяването на подадените предложения.
7. Комисията отстранява от процедурата кандидат, който:
   - е обявен в несъстоятелност/ е в производство по ликвидация / е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - управител или член на управителните органи на кандидат, а в случай, че членове са юридически лица – за техните представители в съответния управителен орган, е лишен от правото да упражнява търговска дейност / е осъден с влязла в сила присъда за престъпление против финансовата, данъчната или осигурителната система, за престъпление по служба или за подкуп, както и за престъпление против собствеността или против стопанството, освен ако не е реабилитиран.
   - не е изготвил и окомплектовал предложението си съгласно изискванията, посочени в документацията за участие;
   - е представил непълно техническо или ценово предложение.
8. Възложителят може да изиска от кандидатите да представят допълнително документи, с които да докажат икономическото и финансовото си състояние, техническите възможности и/или квалификацията си.
9. След разглеждане на получените предложения, Възложителят може еднократно да поиска от кандидатите да представят подобрено ценово предложение.

10. Кандидатите са длъжни в процеса на провеждане на процедурата да уведомяват за всички настъпили промени в обстоятелствата, за които са представили декларация по образец (Приложение № 5 към поканата) - в 7-дневен срок от узнаването им.
11. Лице, което е дало съгласие и фигурира като подизпълнител в офертата на друг кандидат, не може да представя самостоятелна оферта.
12. Когато при изпълнението на договора кандидатът ще използва подизпълнител, предложението трябва да съдържа изискваните документи за идентификация и квалификация и за подизпълнителя.
13. Когато кандидат за участие в процедурата е обединение на юридически лица (консорциум) за всеки от участниците в консорциума се представят документите за идентификация и квалификация, изисквани от участниците в процедурата.
14. Всички кандидати се уведомяват за резултатите от процедурата в срок от три работни дни, считано от датата на решението на Съвета на директорите, с което се одобрява изборът на доставчик, като на избрания за изпълнител кандидат се предлага да сключи договор при условията на подаденото предложение.
15. Когато избраният за изпълнител кандидат откаже, не представи изискваните документи или по друга причина договорът с него не може да бъде подписан, изпълнителният директор предлага на класирания на следващо място кандидат да сключи договор при условията на подаденото предложение или прекратява тази и насрочва нова процедура за избор на доставчик.
16. При подписване на договора кандидатът, определен за изпълнител, представя електронно свидетелство за съдимост за удостоверяване на обстоятелствата, заявени с декларация по образец (Приложение № 5 към поканата). При невъзможност за представяне на електронно свидетелство за съдимост кандидатът представя свидетелство за съдимост или друг еквивалентен документ – сканирани и заверени с квалифициран електронен подпис. Представените документи не се съхраняват от „Информационно обслужване“ АД.