Подписът е заличен на основание чл.2 от ЗЗЛД и във връзка с чл.42, ал.5 от ЗОП.

ОДОБРЯВАМ:

Дата...03.....05.2018 г.,
Гр. София

ПЛАМЕН ПЕШАРОВ
УПРАВИТЕЛ НА „БДЖ-ПП" ЕООД

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

за избор на изпълнител за възлагане на обществена поръчка с предмет:
„Анализ на съответствието на съществуващите системи и процеси в „БДЖ-Пътнически превози" ЕООД („БДЖ-ПП" ЕООД) с изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR) и дефиниране на мерки за привеждане на работните процеси и на информационните системи в съответствие с Регламента"

Възлагането на обществената поръчка има за цел да бъде сключен договор за **„Анализ на съответствието на съществуващите системи и процеси в „БДЖ-Пътнически превози" ЕООД („БДЖ-ПП" ЕООД) с изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR)и дефиниране на мерки за привежда не на работните процеси и на информационните системи в съответствие с Регламента"**, съобразно изискванията на «Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR) и специфичните потребности на Възложителя-„БДЖ-ПП" ЕООД. Въвеждането на регламента ще повиши нивото на сигурност на личните данни и тяхната защита в централната и териториални структури на „БДЖ-ПП" ЕООД, чрез подобряването на ефективността и ефикасността на извършваните дейности, при спазване на изискванията за управление на личните данни.

1. **Място на изпълнение на поръчката** - Централно управление на „БДЖ-ПП" ЕООД и поделенията на регионално ниво при необходимост.
2. **Срок за изпълнение на поръчката** - до 60 (шестдесет) дни след подписване на договора с избрания Изпълнител на обществената поръчка.
3. **Изисквания към изпълнението на поръчката**

GDPR регулацията цели да увеличи правата на гражданите в Европейския съюз в контрола на личните им данни като изисква от организациите да засилят и повишат мерките за тяхната защита.

Основната цел на провеждания анализ е да се установи съответствието и пълнотата на внедрените в организацията контроли за защита на личните данни съгласно изискванията на GDPR регламента.

Основниетапи от изпълнение на поръчкатаса:

- Първоначален анализ на текущото състояние (GAP анализ), който показва доколко вече наличните технологични и организационни мерки покриват изискванията на GDPR Регламента;
- Предоставяне на препоръки за внедряване на организационни и технически мерки и процеси;
- Предоставяне на препоръки за въвеждане на механизми за мониторинг, откриване и рапортуване на изтичане на информация;

Очакваният резултат при изпълнение на поръчката е:

а/ да се направи обобщена обективна оценка на наличните съществуващи системи и

процеси в „БДЖ-ПТ" ЕООД;
б/ да се предостави на Възложителя необходимата информация и препоръки за внедряване на необходимите организационни и технически мерки и процеси, които да доведат до успешно покриване на изискванията на Регламента.
Обект на изследване от Изпълнителя ще бъде -преглед и анализ на наличните управленски процеси и вече въведените в „БДЖ-ПТ" ЕООД вътрешни системи за управление по обхват и функции. За целта е необходимо да бъдат извършени анализи на следните компоненти:

- Налични процедури и инструкции за работа с лични данни;
- Политики по отношение на управлението и защитата на лични данни;
- Описание на ролите и отговорностите на служителите, имащи достъп и боравещи с лични данни;
- Политики и процедури за водене и управление на записи и логове за събития,свързани с достъп до лични данни;
- Технически средства и механизми за съхранение, обработка и сигурно трансфериране на лични данни;
- Докладване и документиране на инциденти, свързани с лични данни;
- Процеси за редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки за защита на личните данни;
- Работа с информационни носители на лични данни;
- Псевдонимизация и Криптография;
- Сигурност на устройствата, съхраняващи, обработващи и трансфериращи лични данни;
- Резервиране и възстановяване на наличността и достъпа до лични данни в случай на инцидент;
- Управление на рисковете, свързани с обработването на лични данни;*
- Други.

**** Под Управление на рисковете, свързани с обработването на лични данни се разбира:***

Оценка на риска на основата на:

- естеството, обхвата, контекста и целите на обработването;

- възможните рискове и тяхната вероятност;

- последиците за правата и свободите на физическите лица и други, съотносими към предмета на поръчката.

Изпълнителят трябва да представи методология на дейностите, свързани с предварителния анализ. Предлаганата методология, трябва да се базира на утвърдени стандарти, добри практики и да покрива изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR).
В резултат на изпълнение на предмета на поръчката, Изпълнителят трябва да предостави Доклад на хартиен и електронен носител, с включени препоръки за коригиращи действия-степенувани и подредени по важност във времето, чието изпълнение ще доведе до постигане на съответствие на Възложителя с изискванията на GDPR.
Изпълнителят е необходимо да представи детайлен план-график за провеждане на дейностите по предмета на поръчката.
Възложителят, с цел успешното изпълнение на предмета на обществената поръчка, ще предостави/ осигури на Изпълнителя:

- Наличната и релевантна информация, поискана от Изпълнителя и необходима за успешното изпълнение на предмета на обществената поръчка;
- Достъп до структурите на Възложителя, включени в предмета и обхвата на

поръчката в рамките на работното време на Възложителя;
• Съдействие от страна на персонала в рамките на работното време на Възложителя.

4. Очаквани резултати:
• Проведен първоначален одит и встъпителен анализ с оценка на текущото състояние на информационните системи, наличните управленски процеси и вече въведените вътрешни системи за управление по обхват и функции в структурите на Възложителя включващ анализ на: текущото състояние на процесите и информационните връзки; вътрешните документи; организацията и извършваните дейности за установяване съответствието на системите и процесите, тяхната последователност и взаимодействие, свързани с управлението на личните данни, съгласно изискванията на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR).
• Предоставени препоръки за внедряване на необходимите организационни и технически мерки и процеси, както и за въвеждане на механизми за мониторинг,откриване и сигнализиране за изтичане на информация.