



**СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № НДМСПО-17-949/28.11.2018 г.
гр. София, 21.12.2018 г.**

ОТНОСНО: Въпроси, свързани с карти „Multisport“.

Комисията за защита на личните данни (КЗЛД) в състав – членове: Цанко Цолов, Цветелин Софрониев и Веселин Целков, на заседание, проведено на 19.12.2018 г., разгледа писмо /вх. № НДМСПО-17-949/2018 г./ от г-жа К.К. – длъжностно лице по защита на данните в „К.“ ЕООД. Г-жа К.К. информира, че дружеството изразява желание да подпише договор с фирма, предлагаща ежемесечни „Multisport“ карти на техните служители за посещение при преференциални условия на фитнес центрове, студиа, плувни комплекси и други спортни съоръжения и дейности. „К.“ ЕООД следва да предостави лични данни на служителите си, желаещи да се възползват от предлаганата услуга, за целите на издаване на картите, като на същите ежемесечно ще се удържат суми от трудовото им възнаграждение.

Въпросът, който поставя г-жа К.К. е дали в конкретния случай фирмата, предлагаща услугата, се явява обработващ лични данни и следва ли в договора, сключен между двете дружества или в друг правен акт да се уреди обработването на лични данни, съгласно изискванията на чл. 28, § 3 от Общия регламент относно защитата на данните.

Правен анализ:

Поради постъпилите множество сходни запитвания и разпространеността на услугата, от съществено значение е определянето на правоотношенията между участниците, както и основанията за обработване на личните данни на служителите, ползватели на услугата „Multisport“ карта.

Съгласно чл. 4, т. 7 от Общия регламент относно защитата на данните (Регламент (ЕС) 2016/679) „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка,

администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.

Качеството администратор е пряко следствие от обстоятелството, че конкретно лице е избрало да обработва лични данни за свои цели или за цели, които са регламентирани с нормативен акт. При това положение, извън случаите, когато това е законово определено, администраторът сам взема решение относно необходимостта от събиране на лични данни, категориите лични данни, дали те да бъдат променяни в хода на обработването, къде и как тези данни да бъдат използвани и с каква цел, дали данните да бъдат разкрити на трети страни и кои да бъдат те, както и за колко време те ще бъдат съхранявани, и кога и по какъв начин да бъдат унищожени.

В допълнение, Регламентът вменява на администратора определен кръг от задължения. Той трябва да предприеме подходящи технически и организационни мерки, свързани със сигурността на данните, като вземе предвид естеството, обхвата, контекста и целите на обработването на данните, както и съществуващите рискове за правата и свободите на субектите на данните. Освен това, съгласно разпоредбата на чл. 30, § 1 от Регламент (ЕС) 2016/679, администраторът поддържа регистър на дейностите по обработване, за които отговаря. Този ангажимент произтича от принципа за отчетност и необходимостта администраторът във всеки един момент да бъде способен да докаже, че спазва изискванията, залегнали в регламента.

„Обработващ лични данни“ е *„физическо или юридическо лице, публичен орган, агенция или структура, която обработва лични данни от името на администратора“* (чл. 4, т. 8 от Регламент (ЕС) 2016/679).

Основната разлика между администратор и обработващ се състои в това, че вторият не действа самостоятелно, а от името на администратора на лични данни. Техните отношения се уреждат с договор, който регламентира предмета, срока на действие по обработването, естеството и целта на обработването, вида лични данни и задълженията и правата на администратора, вкл. да извършва проверки (одити).

Общият регламент въвежда и специфични задължения за обработващия данните, които не се ограничават само и единствено до осигуряване на сигурност на данните. Така например, той е длъжен да обработва лични данни само по документално нареждане от страна на администратора. В случаите, когато е необходимо назначаването на друг обработващ данните, това става само с изричното писмено разрешение на администратора. Подобно на администратора, съгласно чл. 30, § 2 от Общия регламент, обработващият също поддържа регистър на дейностите по обработване, за които отговаря.

В допълнение, с оглед още по-голяма яснота, разпоредбата на чл. 28, § 10 от Общия регламент изрично предвижда, ако обработващият започне сам да определя целите и средствата на обработване, той автоматично започва да се счита за администратор.

Принципът на отчетност, визиран в чл. 5, § 2 от Регламент (ЕС) 2016/679, изисква от участниците в търговския и гражданския оборот, вземайки предвид своята дейност, сами да определят какви са техните правоотношения във връзка с обработваните от тях лични данни – самостоятелни администратори, администратор и обработващ по смисъла на чл. 28 или съвместни администратори по чл. 26 от Общия регламент. Техният избор следва да гарантира не само формално, но и по същество съответствие с изискванията на Регламент (ЕС) 2016/679 и съответно ефективна защита на правата на субектите на данни. Също така, следва да се има предвид, че предоставянето на услуги, при които обичайно се обменят лични данни между възложителя и изпълнителя, не води автоматично до възникване на отношения между администратор и обработващ по смисъла на чл. 28 от Регламента.

Участниците в конкретното правоотношение са три:

- Фирмата, предлагаща „Multisport“ услуга;
- „К.“ ЕООД в качеството си на работодател/администратор на лични данни;
- Служителите на „К.“ ЕООД като ползватели на предлаганата услуга.

„К.“ ЕООД е администратор на лични данни на собствено основание и обработва лични данни на служителите си за целите на трудовото правоотношение с тях. Като работодател дружеството желае да мотивира служителите си като им предостави възможност за физическа активност и здравословен начин на живот, който несъмнено би довел до повишаване на продуктивността им.

От друга страна фирмата, предлагаща услугата „Multisport“, е дружество, чиято основна цел е генериране на търговска печалба, като тя също е администратор на лични данни на собствено основание.

Основна характеристика на отношението администратор – обработващ лични данни е, че вторият обработва данните само по нареждане на администратора /арг. чл. 28, § 3, б. „а“ вр. с чл. 29 от Общия регламент/.

В отношението помежду си двете дружества обработват личните данни за различни цели, съхраняват ги за различни срокове, предават ги на различни получатели, прилагат различни технически и организационни мерки за защита и т.н.

В този ред на мисли може да се направи извод, че визираните характеристики за обработване на лични данни не са унифицирани, следователно същите не могат да бъдат предмет на договаряне и възлагане от администратор към обработващ по смисъла на чл. 28, § 3 от Регламент (ЕС) 2016/679. В конкретния случай правоотношението между „К.“ ЕООД и

фирмата, предлагаща „Multisport“ услуга е между два самостоятелни администратора на лични данни.

Обработването на лични данни е допустимо, когато е налице основание за законосъобразност по смисъла на чл. 6, както и при спазване на принципите за обработка, прогласени в чл. 5 на Общия регламент.

„К.“ ЕООД в качеството си на работодател, предавайки лични данни на служителите си на фирмата, предлагаща „Multisport“ услугата, извършва действие по допълнително обработване на лични данни за цели, различни от първоначалните (за целите на трудовото правоотношение). С оглед на факта, че услугата „Multisport“ е **придобивка с незадължителен характер** за служителите, най-логично е като основание за предаване на личните данни на фирмата, предлагаща услугата, да се използва „съгласие“ по смисъла на чл. 6, § 1, б. „а“ вр. с чл. 4, т. 11 от Общия регламент. В случая служителите имат истински и свободен избор, а също така и възможност за отказ от услугата, без това да доведе до неблагоприятни последици за тях в рамките на трудовото правоотношение /арг. съобр. 42, последно изречение от Общия регламент/. Договорното основание не следва да е приложимо с оглед на факта, че служителите (субекти на данни) не са страна по договора между работодателя и фирмата, предлагаща „Multisport“ услуга. Нещо повече, в тези облигационни отношения, те разполагат с директното право да изискват изпълнение на договореното в тяхна полза, но не и да претендират за разтрогване или изменение на договора, следователно не са част от процеса на доброволното волеизявление (съгласие) за сключване и определяне условията на договора, включително и по отношение на обработката на лични данни.

В допълнение, следва да се отбележи и разпоредбата на чл. 272 от Кодекса на труда (КТ), респ. чл. 72 от Закона за държавния служител (ЗДСл), съгласно която без **съгласието** на работника или служителя не могат да се правят удръжки от трудовото му възнаграждение освен за изчерпателно изброените случаи, сред които не попада удръжката за „Multisport“ карта.

Възможни са различни отклонения в зависимост от регулирането на отношенията в договора между фирмата, предлагаща „Multisport“ услугата и работодателя, като плащането на цената на услугата може да се разпределя между работодател и служител или да се поема изцяло от служителя или работодателя.

Допустимо е ползватели на услугата да бъдат и трети лица, напр. съпрузи и деца на служителя. Техните лични данни също следва да се обработват на основание съгласие.

Във връзка с гореизложеното, „К.“ ЕООД следва да спазва характеристиките на съгласието, визирани в чл. 4, т. 11 и също така да изпълни задължението си за предоставяне на информация по смисъла на чл. 13 и чл. 14 от Регламент (ЕС) 2016/679.

С оглед на гореизложеното и на основание чл. 58, § 3, б. „б“ от Регламент (ЕС) 2016/679, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. „К.“ ЕООД, в качеството си на администратор на лични данни, може да предостави лични данни на свои служители на фирмата, предлагаща услугата „Multisport“ карта, при наличие на изрично изразено съгласие от тяхна страна по смисъла на чл. 6, § 1, б. „а“ вр. с чл. 4, т. 11 от Регламент (ЕС) 2016/679.

2. Допустимо е ползватели на услугата да бъдат и трети лица, напр. съпрузи и деца на служителя, като по отношение на техните лични данни също следва да се прилага съгласието като основание за законосъобразност на обработването.

3. Доколкото „К.“ ЕООД и фирмата, предлагаща „Multisport“ услугата, обработват личните данни за различни цели, съхраняват ги за различни срокове, предават ги на различни получатели, прилагат различни технически и организационни мерки за защита и т.н., същите се явяват самостоятелни администратори на лични данни, съответно не попадат в хипотезата на отношения администратор – обработващ по смисъла на чл. 28 от Общия регламент.

4. При обработване на личните данни и двете дружества следва стриктно да спазват задължението си за предоставяне на информация по реда на чл. 13 и чл. 14, в съответствие с изискванията на чл. 12 от Регламент (ЕС) 2016/679.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Цветелин Софрониев /п/

Веселин Целков /п/