КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

С Т А Н О В И Щ Е

НА

КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

рег. № НДМСПО-01-1174/10.12.2018 г.

гр. София, 11.01.2019 г.

ОТНОСНО: Искане за становище във връзка с определяне на качествата администратор и обработващ лични данни.

Комисията за защита на личните данни (КЗЛД) в състав – членове: Цанко Цолов, Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 09.01.2019 г., разгледа искане за становище /вх. № НДМСПО-01-1174/10.12.2018 г./ от „Б.С.М.Ц." ООД, гр. В., във връзка с възникнал казус при определяне на качествата „администратор" и „обработващ" лични данни, касаещ пораждането на правоотношение със застрахователно дружество, на чиито клиенти по застрахователни договори за обезпечаване на задължения, медицинският център предоставя услуги, а именно диференцирани прегледи и изследвания.

Медицинският център изразява становище, че в отношенията си със застрахователи действа в качеството на обработващ лични данни. В писмото се изтъква, че с едно от застрахователните дружествата имат спор, като последното счита, че по аналогия следва да се приложи становището на КЗЛД (рег. № НДМСПО-17-604/20.06.2018 г.) по казуса с пощенския оператор „С." АД и медицинският център би следвало да има качеството на администратор на лични данни.

Поставя се въпросът, в какво качество (администратор или обработващ) медицинският център следва да сключи договор със застрахователното дружество.

Правен анализ:

Съгласно легалната дефиниция, визирана в 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, пар. 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, т.е. **последиците от обработването на личните данни, настъпват директно в правната сфера на администратора.** Техните отношения се уреждат с договор ли с друг правен акт съгласно правото на ЕС или правото на държава членка, който регламентира предмета и срока на действие, естеството и целта на обработването, вида лични данни и категориите субекти на данни и правата и задълженията 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 документирано нареждане от страна на администратора /арг. чл. 28, пар. 3, б. „а“ вр. с чл. 29 от Общия регламент/. 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, пар. 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, пар. 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, пар. 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.

Поначало администраторът на лични данни може да „възлага“ на обработващ дейности по обработка, за които самият той има **правна възможност** да извършва, но поради различни причини от организационно, техническо, финансово или друго естество е преценил, че е по-подходящо да се извършват от фигурата на т.нар. обработващ.

Класически пример за възлагане на дейност по обработка на лични данни на обработващ, е задължението на работодателя за осигуряване на обслужване на работещите от служби по трудова медицина. Съгласно разпоредбата на чл. 2, ал. 2 от *Наредба № 3 от 25.01.2008 г.за условията и реда за осъществяване дейността на службите по трудова медицина*, същите се създават от работодателя в рамките на предприятието или от самостоятелни юридически или физически лица, регистрирани по Търговския закон, по Закона за кооперациите или по Закона за юридическите лица с нестопанска цел. Нещо повече, в ал. 4 е предвидено, че когато за работодателя е практически невъзможно сам да създаде служба по трудова медицина, той сключва

договор със служба, регистрирана по реда на чл. 25в от Закона за здравословни и безопасни условия на труд (ЗЗБУТ).

В конкретния случай, дейността по обработване на лични данни във връзка с извършване на прегледи и изследвания не би могла да се извърши **„от името“** на застрахователя (администратор), поради факта, че същите не могат да бъдат реализирани от него, а само от организация, имаща качеството „лечебно заведение“ по смисъла на Закона за лечебните заведения. В допълнение, видно от разпоредбата на чл. 95, ал. 1, т. 2 от Закона за лечебните заведения, същите могат да сключват договори със застрахователи. Посочените договори би следвало да се сключват между страните в качеството им на администратори на лични данни, а не на администратор – обработващ по смисъла на чл. 28 от Общия регламент.

Аналогична е тезата, изразена от КЗЛД в становищата ѝ относно качествата „администратор“ и „обработващ“ в пощенската и банковата дейност, като същите са публикувани на официалната ѝ интернет страница.

От друга страна и не на последно място, специалното законодателство в сферата на здравеопазването (законово и подзаконово), предвижда редица задължения, мерки, механизми, ред и условия за защита на здравната информация, съдържаща лични данни, които не могат да бъдат дерогирани с договор по смисъла на чл. 28 от Общия регламент.

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. В конкретния случай, дейността по обработване на лични данни във връзка с извършване на прегледи и изследвания не би могла да се извърши от името на застрахователя (администратор), поради факта, че същите не могат да бъдат реализирани от него, а само от организация, имаща качеството „лечебно заведение“ по смисъла на Закона за лечебните заведения.

2. Специалното законодателство в сферата на здравеопазването (законово и подзаконово), предвижда редица задължения, мерки, механизми, ред и условия за защита на здравната информация, съдържаща лични данни, които не могат да бъдат дерогирани с договор по смисъла на чл. 28 от Общия регламент.

3. Участниците в търговския и гражданския оборот, вземайки предвид своята дейност, както и приложимото спрямо нея законодателство, следва 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 правоотношение между администратор и обработващ по смисъла на чл. 28 от Регламента.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/