



СТ А Н О В И Щ Е
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
рег. № НДМСПО-01-1180/11.12.2018 г.
гр. София, 04.02.2019 г.

ОТНОСНО: Изясняване на връзката „администратор – обработващ“ между НЗОК и аптеки, сключили договори с нея, по повод прилагането на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

Комисията за защита на личните данни (КЗЛД) в състав – членове: Цанко Цолов, Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 30.01.2019 г., разгледа искане за становище /вх. № НДМСПО-01-1180/11.12.2018 г./ от г-жа В.В.К., в качеството ѝ на управител на „С.“ ЕООД. Дружеството е с предмет на дейност търговия на дребно с лекарствени продукти. Г-жа В.В.К. информира, че „С.“ ЕООД е едноличен собственик на капитала на 11 други дружества със същия предмет на дейност. В рамките на обичайната си търговска дейност „С.“ ЕООД и дъщерните му дружества са открили и поддържат работата на 31 броя аптеки под търговското наименование „С.“ (Аптеките).

С оглед на горното, ръководството на „С.“ ЕООД цели да инициира кореспонденция между Аптеките и НЗОК, чрез която да бъде изяснено каква роля заема НЗОК спрямо Аптеките по отношение на личните данни на пациенти и медицински специалисти, съдържащи се в рецептите, които Аптеките изпълняват и чиито лични данни Аптеките изпращат на НЗОК по силата на Договор за отпускане на лекарствени продукти, медицински изделия и диетични храни за специални медицински цели за домашно лечение, заплащани напълно или частично от НЗОК/РЗОК (Договора).

Г-жа В.В.К. посочва следните факти и обстоятелства, които според нея следва да се вземат предвид:

1. чл. 7 от Наредба № 4 от 4.03.2009 г. за условията и реда за предписване и отпускане на лекарствени продукти (Наредба 4) съдържа нормативните изисквания за съдържанието на

рецептата. Сред тези изисквания се включват лични данни като имената на лекаря, който изписва рецептата, имена, възраст, адрес и други лични данни за пациента.

2. При приемането на рецептите работещите в Аптеките магистър - фармацевти правят различни видове обработки на тези данни – проверяват ги, съхраняват ги, изпращат ги на НЗОК.

3. Отношенията между НЗОК и Аптеките се регулират с договор, като чл. 20, ал. 1, т. 3 от Договора за 2018 г. например предвижда, че Аптеките трябва да представят на НЗОК екземпляри от изпълнените рецепти. Аптеките не могат да договарят условията на този договор и той се подписва в текста, който е приет по силата на чл. 45, ал. 15 от Закона за здравното осигуряване.

Съгласно действащите разпоредби на Общия регламент относно защитата на данните, НЗОК и Аптеките са администратори на лични данни, всеки действащ на собствено основание, за различните видове обработки, които правят. В конкретния случай на подписан Договор между аптека и НЗОК обаче аптеката, по силата на Договора, е длъжна да изпраща на НЗОК рецептурни бланки и различни отчети, които съдържат лични данни. Дори и типовия софтуер, който аптеките ползват, трябва да бъде съобразен с изискванията на НЗОК - чл. 14 от Договора.

Разбирането на дружеството е, че в случаите, когато аптека обработва лични данни, които обработки са ѝ възложени с Договора, тя действа като обработващ на НЗОК, а последната е администратор. Това е така, защото обработките на лични данни, предвидени в договора, се правят от аптеката. Аптеката не би ги правила, ако не ѝ бяха възложени с Договора. Целите и средствата за обработката (включително софтуера) се определят от НЗОК, а Аптеките са просто изпълнител.

С оглед на горното и предвид отношенията, които Аптеките имат с НЗОК, г-жа В.В.К. моли КЗЛД да се произнесе по отношение на обработката на лични данни – изпращане на рецепти и отчети съдържащи лични данни от Аптеките към НЗОК и други обработки по силата на Договора. В допълнение, молбата е да бъдат информирани дали с оглед на така представените отношения Аптеките следва да бъдат обработващи на лични данни по отношение на НЗОК за тези конкретни обработки, произтичащи от Договора.

Правен анализ:

Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните), който се прилага от 25 май 2018 г., е нормативният акт, определящ правилата, свързани със защитата на личните данни на физическите лица при тяхното обработване. Общият регламент надгражда предишния режим за защита на данните, въведен от Директива 95/46/ЕО, транспонирана в българския Закон за защита на личните данни от 2002 г., като в същото време отчита динамиката на развитието на новите технологии и на дейностите по обработка на лични данни.

Концепцията за администратор и обработващ лични данни е въведена с Директива 95/46/ЕО и е доразвита с новата европейска правна рамка за защита на личните данни.

Съгласно легалната дефиниция, визирана в чл. 4, т. 7 от 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 юридическо или физическо 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 или модифицирани 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.

От друга страна, **обработващият** 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 фигурите на администратора и обработващия се състои в това, че вторият не действа самостоятелно, а от името на администратора на лични данни, т.е. **правните последиците от обработването на личните данни настъпват директно в правната сфера на администратора.**

Отношенията администратор – обработващ се уреждат с договор или 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).

Поначало, администраторът може да възлага на обработващ дейности по обработка на лични данни, 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 обработващия. В този ред на мисли 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 (теза изразена в редица становища на КЗЛД).

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, § 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, § 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.

Разпределението на ролите и отговорностите между администратора и обработващия има една основна цел, а именно да гарантира, че обработването на лични данни протича в съответствие с изискванията на Регламент (ЕС) 2016/679 и съответно осигурява защита на правата на физическите лица – субекти на данни.

Правоотношението между аптеките и НЗОК е строго регулирана дейност, уредена със Закона за здравното осигуряване (ЗЗО) и Наредба № 4 от 4 март 2009 г. за условията и реда за предписване и отпускане на лекарствени продукти, издадена от министъра на здравеопазването.

В тази връзка, разпоредбата на чл. 46, ал. 2 от Наредба № 4 предвижда, че отпускането на лекарствени продукти от аптеки, работещи по договор с НЗОК, се извършва в съответствие с тази наредба и с условията и реда за сключване на индивидуални договори по чл. 45, ал. 15 от ЗЗО.

Посочените договори са с предварително и едностранно зададена форма и съдържание, което не подлежи на изменение от страна на аптеките. За страните по договора (Аптеките и НЗОК) са предвидени права и задължения, които са в пряка връзка с реализирането на предмета на договора, а именно отпускането на лекарствени продукти.

Няма съмнение, че изпълнението на задълженията за страните по договора е свързано с дейности по обработка на лични данни на пациенти, медицински специалисти и фармацевти, чиито данни следва да се предоставят под формата на различни документи на НЗОК. Договорът предвижда задължения за аптеките, които обаче не следва да се квалифицират като „възлагане“, което е основният отличителен белег за отношението администратор – обработващ лични данни /арг. чл. 4, т. 8 от Регламент (ЕС) 2016/679/. Напротив, въпросните задължения имат публичноправен характер за аптеката, независимо че същата е търговско дружество. На практика, независимо от наименованието му, договорът между НЗОК и съответната аптека има характер на **нормативен административен акт**, който допълва императивната правна уредба на тази строго регулирана дейност. Аналогична е ситуацията и с Националния рамков договор, който по силата на чл. 4а от ЗЗО също се явява нормативен административен акт, който има действие на територията на цялата страна за определен срок и е задължителен за НЗОК, изпълнителите на медицинска помощ, осигурените лица и осигурителите.

В допълнение, специалното законодателство в сферата на здравеопазването (законово и подзаконово), предвижда редица задължения, мерки, механизми, ред и условия за обработка и защита на личните данни, които не могат да бъдат дерогирани с договор между администратор и обработващ 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. Договорът между НЗОК и аптеките, който урежда отношенията между тях на основание Закона за здравното осигуряване и Наредба № 4 от 4 март 2009 г. за условията и реда за предписване и отпускане на лекарствени продукти, издадена от министъра на здравеопазването, не води до възникване на правоотношение администратор – обработващ лични данни по смисъла на чл. 28 от Регламент (ЕС) 2016/679. Въпросният договор има характер на нормативен административен акт, който допълва императивната правна уредба в тази област.

2. По принцип дружествата, които предоставят услуги при условията на строга и изчерпателна законова регламентация, въз основа на лицензия или аналогично индивидуално

разрешение от държавата и под контрола на изрично определени публични органи, не биха могли да се разглеждат като обработващи лични данни, а като самостоятелни администратори. Наред с това, специалното законодателство в сферата на здравеопазването предвижда редица задължения, мерки, механизми, ред и условия за обработка и защита на личните данни, които не могат да бъдат дерогирани с договор по смисъла на чл. 28 от Общия регламент.

ЧЛЕНОВЕ:

Цанко Цолов /п/

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/