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-01-873/10.08.2018 г.
гр. София, 21.09.2018 г.

ОТНОСНО: Искане за становище по прилагането на Регламент (ЕС) 2016/679 от „УниКредит Булбанк" АД

Комисията за защита на личните данни (КЗЛД) в състав – членове: Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 19.09.2018 г., разгледа искане за становище /вх. № НДМСПО-01-873/10.08.2018 г./ от „УниКредит Булбанк" АД, в което се поставят следните въпроси относно приложението на Регламент (ЕС) 2016/679:

1. Допустимо ли е съвместни администратори да разчитат на едно волеизявление за предоставяне на съгласие от страна на субекта, чиито данни обработват, с цел предлагане на директен маркетинг.

2. Какво качеството има банката във връзка с противоречивото тълкуване на правните фигури „администратор" и „обработващ лични данни" в контекста на взаимоотношенията ѝ с клиентите.

Във връзка с привеждането на дейността си в съответствие с Регламент (ЕС) 2016/679, „УниКредит Булбанк" АД се сблъсква с противоречиво тълкуване от страна на своите клиенти на качеството на страните в отношенията, свързани с предоставянето на банкови услуги – администратор и обработващ. Клиенти на банката изискват подписването на споразумение, според което клиентът има качеството на администратор по отношение на данните, които предоставя на „УниКредит Булбанк" АД, визирайки, че банката има качеството на обработващ данните. Основният им аргумент в тази насока е, че сключваните между страните договори за банкови услуги, по които клиентът има качеството „възложител", а „УниКредит Булбанк" АД на „изпълнител", обуславят и поставянето им в позиция „администратор" (клиент) и „обработващ" (банката).

От своя страна, „УниКредит Булбанк" АД не споделя това тълкуване на Общия регламент, като счита, че при осъществяването на дейността по предоставяне на банкови услуги на физически и юридически лица, тя притежава качеството и задълженията на

„администратор“ на собствено основание по отношение на събираните и обработваните лични данни. В допълнение, предоставянето на тези специфични услуги може да бъде извършено единствено при наличие на съответния лиценз, т.е. обработването на данни се извършва на собствено основание, а не от името на клиента.

При преценката относно качеството „администратор“, „УниКредит Булбанк“ АД е използвала разясненията, съдържащи се в Становище 1/2010 на Работната група по чл. 29 от Директива 95/46/ЕО относно понятията „администратор“ и „обработващ личните данни“, в което недвусмислено банките са определени като администратори на лични данни при извършване на финансови транзакции.

Във връзка с гореизложеното, както и с цел избягване на незаконосъобразно поведение и несигурност по отношение на относимите към страните на банковите услуги задължения, „УниКредит Булбанк“ АД моли за становище по горепосочените въпроси.

<u>Правен анализ</u>:

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.

1. Фигурата на „съвместни администратори“ е нова и е въведена с чл. 26 от Общия регламент, съгласно който, когато двама или повече администратори съвместно определят целите и средствата на обработването, те имат качеството на съвместни администратори. Посредством договор помежду си те трябва да определят по прозрачен начин отговорностите си за изпълнение на задълженията по Регламента и по-специално по отношение упражняването на правата на субектите на данни и съответните им задължения за предоставяне на информацията по чл. 13 и 14 от Регламента. Договорът трябва да отразява съответните роли и връзки на съвместните администратори спрямо субектите на данни, като съществените характеристики на този договор следва да са достъпни за субекта на данни. Препоръчително е в договора да се посочи точка за контакт за субектите на данни. В допълнение, независимо от условията на договора, субектите на данни могат да упражняват своите права по отношение на всеки и срещу всеки от администраторите, в т. ч. и правото на оттегляне на съгласието по всяко време.

Във връзка с гореизложеното, може да се направи извод, че няма нормативна пречка съвместни администратори да използват „едно съгласие“ от страна на субекта, чиито данни обработват с цел предлагане на директен маркетинг, доколкото са изпълнени следните условия:

- съгласието следва да отговаря на специфичните изисквания на чл. 4, т. 11 и чл. 7 от Регламента, а именно да е свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, дадено посредством изявление или ясно потвърждаващо действие, което може да бъде оттеглено по всяко време;

- да са изпълнени изискванията за прозрачност по чл. 5, параграф 1, б. „а“, чл. 13 и чл. 26, параграф 1 от Регламента, като субектът на данните следва да е информиран както за целите на обработване, така и за обхвата на предоставяното от него съгласие.

2. 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 на чл. 4, т. 7 от Общия регламент, **администратор** е *„физическо или юридическо лице, публичен орган, агенция или държавна 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 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, 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 действа не 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, 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.

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.

Обществените отношения, свързани с банковата дейност и предоставянето на банкови услуги на територията на Република България, са изчерпателно уредени в Закона за кредитните институции (ЗКИ), Закона за Българската народна банка (ЗБНБ), Закона за платежните услуги и платежните системи (ЗПУПС) и съответните подзаконови нормативни актове. Най-общо банкови услуги включват приемане на депозити и даване на заеми, но наред с това банките предлагат и редица платежни услуги. В допълнение, банките подлежат на лицензиране и надзор от Българската народна банка (БНБ).

Във връзка с гореизложеното, следва да се отбележи, че банковата дейност е строго нормативно регламентирана, като в специалното законодателство са уредени целите на

обработването на лични данни; категориите лични данни; получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни; сроковете за съхранение и т.н. Поради факта, че визирани характеристики за обработване на лични данни са нормативно определени в банковото законодателство, същите не могат да бъдат предмет на договаряне по смисъла на чл. 28, пар. 3 от Регламент (ЕС) 2016/679.

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.

Друг важен аспект, на който трябва да се обърне особено внимание, е високата степен на нормативно регулиране на дейността на банките. На практика това означава, че както те самите, така и техните клиенти имат ограничена възможност да определят самостоятелно целите и средствата за обработване на лични данни при предоставяне на банкови услуги. Това обстоятелство трябва да се отчита в пълна степен при сключване на договори с други администратори на лични данни, за да не се допусне нарушение на приложимата правна рамка.

Във връзка с изложените по-горе доводи, без да се извежда като абсолютно правило, може да се приеме, че дружествата, които предоставят услуги при условията на строга и изчерпателна нормативна регламентация, въз основа на лицензия или аналогично индивидуално разрешение от държавата и под контрола на изрично определени публични органи, принципно не биха могли да се разглеждат като обработващи лични данни, а като самостоятелни администратори. Примери за такива администратори са банките, пощенските оператори, застрахователните дружества и др. В тези случаи възложителят по договор за услуга не би могъл да укаже на предоставящия услугата как точно да обработи предоставените от него лични данни, тъй като и двете страни са длъжни да спазват съответното специално законодателство, в т.ч. съдържащи те се в него разпоредби относно обработването на лични данни.

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

СТАНОВИЩЕ:

1. Няма нормативна пречка съвместни администратори да използват „едно съгласие“ от страна на субекта, чиито данни обработват с цел предлагане на директен маркетинг, при условие, че са спазени специфичните изисквания по отношение на съгласието по чл. 4, т. 11 и чл. 7 от Регламент (ЕС) 2016/679, както и задължението за прозрачност на обработването по силата на чл. 5, параграф 1, б. „а“, чл. 13 и чл. 26, параграф 1 от Общия регламент.

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. Примери за такива администратори са банките, пощенските оператори и застрахователните дружества.

Предвид многообразието от обществени отношения и в съответствие с принципа за отчетност, регламентиран в чл. 5, пар. 2 от Регламент (ЕС) 2016/679, участниците в търговския и гражданския оборот следва сами да определят във всеки отделен случай какви са техните правоотношения във връзка с обработваните от тях лични данни – самостоятелни администратори, администратор и обработващ или съвместни администратори. Техният избор не следва да е формален и трябва да гарантира в най-голяма степен съответствие с изискванията на Регламент (ЕС) 2016/679 и ефективна защита на правата на субектите на данни.

ЧЛЕНОВЕ:

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/