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

СТАНОВИЩЕ
НА
КОМИСИЯТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Рег. № НДМСПО-01-264/2018 г.
гр. София, 22.11.2018 г.

ОТНОСНО: ***Правила за небанкови финансови институции за еднозначно разпознаване на физически лица във виртуална среда при предоставяне на финансови услуги от разстояние***

Комисията за защита на личните данни (КЗЛД, Комисията) в състав: членове: Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 21.11.2018 г., разгледа преписка с рег. № НДМСПО-01-264/2018 год. от г-н П.Д. – Управител на „Б.Ф." ООД, по въпроси, касаещи правила за небанкови финансови институции за еднозначно разпознаване на физически лица във виртуална среда при предоставяне на финансови услуги от разстояние.

„Б.Ф." ООД е небанкова финансова институция, вписана с рег. № ****** в Регистъра на финансовите институции по чл. 3а от Закона за кредитните институции (ЗКИ) на БНБ. Дружеството предоставя финансови услуги от разстояние и по-специално потребителски кредити на физически лица. Кандидатстването и отпускането на заемите на потребителите се осъществява неприсъствено съгласно Закона за предоставяне на финансови услуги от разстояние и Закона за потребителските кредити. Правните изявления при кандидатстване и отпускане на кредити на физическите лица се разменят и удостоверяват чрез усъвършенстван електронен подпис по чл. 13, ал. 2 и ал. 4 от ЗЕПЕУУ, създаден чрез средства за индивидуализация - телефон и електронна поща, ведно с персонален код, на които е придадено значение на саморъчен подпис относно обвързаните с тях електронни изявления.

Като финансова институция дружеството попада в кръга на лицата, които трябва да прилагат мерки за предотвратяване изпирането на пари и финансирането на тероризма. Но част от отпусканите заеми са малки суми, чиито стойности са значително под праговете, изискващи специални мерки за идентификация съгласно ЗМИП и ЗМФТ.

При извършване дейността на финансовата институция се идентифицират практически затруднения, свързани с еднозначно разграничаване на едно лице от друго във виртуална среда. Дори да се извърши контрол и проверка на идентификационните данни, предоставени от клиента, не може да се елиминира рискът от заявяване и ползване на финансови услуги от лица чрез т.нар. „кражба на самоличност“, когато едно лице се представя за друго.

Законът за електронната идентификация има за цел да уреди обществените отношения, свързани с електронното разпознаване на физически лица, но влизането му в действие е отложено за 01.01.2019 г. Към настоящия момент правната и икономическа среда, в която оперират небанковите финансови институции, предоставящи дистанционно услуги за потребителско кредитиране на физически лица, остава несигурна и заплашена от неспецифични непазарни рискове.

Обективните затруднения при еднозначно разпознаване на физическите лица във виртуална среда са предпоставка за измами и други форми на забранено от закона поведение от страна на недобросъвестни лица, които изискват специални мерки, за да не подкопават доверието и икономическата ефективност на кредитната дейност на небанковите финансови институции.

Същевременно с цел привеждане в съответствие с изискванията на Регламент (ЕС) 2016/679 (GDPR) небанковите финансови институции трябва да сведат събирането и обработването на личните данни на физическите лица до минимум, в съответствие с целите на предоставяните услуги. Обработването на по-голям обем лични данни на потребителите с цел защита икономическите интереси на администратора може да накърни принципа на пропорционалност при обработването.

Изложеното има за цел да обоснове необходимостта от становище на Комисията за защита на личните данни по следните въпроси:

- При прилагането на Регламент (ЕС) 2016/679 (GDPR) от 25 май 2018 г. остава ли актуално и приложимо становището, изразено в Решение № Ж-39/09.06.2016 г. на КЗЛД за това, че небанкова финансова институция, като администратор на лични данни, е задължена при идентификация на клиента или проверката й, да изиска официален документ за самоличност, съдържащ снимката му, какъвто документ е личната карта, както и да направи копие от него и да го съхранява пет години.

- При установяване, че физическо лице е заявило и/или получило паричен заем по реда на Закона за предоставяне на финансови услуги от разстояние от небанкова финансова институция, чрез т.нар. „кражба на самоличност“, когато едно лице се

представя за друго, задължена ли е небанковата финансова институция, като администратор на лични данни, да уведомява надзорния орган за нарушаване сигурността на личните данни съгласно изискванията на чл.33 от Регламент (ЕС) 2016/679 (GDPR).

В тази връзка г-н П.Д., моли КЗЛД да изрази становище и указания, адресирани до финансовите институции, относно обработването на лични данни на физическите лица при предоставяне на финансови услуги от разстояние, с цел преодоляване на специфичните рискове, свързани с еднозначното разграничаване на физическите лица във виртуална среда.

Правен анализ:

Законът за кредитните институции (ЗКИ) дефинира дейностите и присъщите по предмет на дейност задължения на банковите и небанковите финансови институции. Небанковите финансови институции, по смисъла на чл. 3, ал. 1 от ЗКИ имат право да извършват като основна дейност придобиване на участия в кредитна институция или в друга финансова институция, отпускане на кредити със средства, които не са набрани чрез публично привличане на влогове или други възстановими средства, извършване на платежни услуги по смисъла на Закона за платежните услуги и платежните системи (ЗПУПС) и др. До влизането в сила на чл. 100, ал. 1 от ЗПУПС, по силата на Окончателните насоки относно сигурността на плащанията в интернет на Европейския банков орган, финансовата институция трябва да проведе задълбочено удостоверяване на автентичността на клиента с цел оторизиране на плащания в интернет от страна на клиента и с цел издаването или изменението на електронни мандати за директен дебит. По смисъла на делегирания Регламент на Комисията за допълнение на Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета по отношение на регулаторните технически стандарти за задълбоченото установяване на идентичността на клиента и общите и сигурни отворени стандарти на комуникация, изискванията за идентификация са значително завишени, особено когато клиентът извършва действие от разстояние, при което би могло да възникне риск от измама при плащането или друга злоупотреба. По смисъла на т. 63 от Допълнителните разпоредби на ЗПУПС установяването на идентичността е „процедура, която позволява на доставчика на платежни услуги да провери самоличността на ползвателя на платежни услуги, включително използването на персонализираните средства за сигурност на ползвателя“.

Извън задълженията, вменени с оглед упражняване дейността на финансовата институция, Законът за мерките срещу изпирането на пари (ЗМИП) определя мерките за превенция на използването на финансовата система за целите на изпирането на пари, както и организацията и контролът по тяхното изпълнение. В чл. 3 от ЗМИП са разписани мерките за превенция на използването на финансовата система за целите на изпирането на пари и те са:

1. комплексна проверка на клиентите;

2. събиране и изготвяне на документи и друга информация при условията и по реда на този закон;

3. съхраняване на събраните и изготвените за целите на този закон документи, данни и информация;

4. оценка на риска от изпиране на пари;

5. разкриване на информация относно съмнителни операции, сделки и клиенти;

6. разкриване на друга информация за целите на този закон;

7. контрол върху дейността на задължените субекти по раздел II от тази глава;

8. обмен на информация и взаимодействие на национално равнище, както и обмен на информация и взаимодействие между дирекция „Финансово разузнаване“ на Държавна агенция „Национална сигурност“, звената за финансово разузнаване на други държави и юрисдикции, както и с компетентните в съответната сфера органи и организации на други държави.

Горецитираните мерки за превенция и контрол на изпълнението им са задължителни за субектите, изброени в чл. 4 от същия закон. В чл. 4, ал. 1 като задължени субекти, са отбелязани Българската народна банка и кредитните институции, които извършват дейност на територията на Република България по смисъла на Закона за кредитните институции. „Б.Ф.“ ООД е небанкова финансова институция, вписана с рег. № ****** в Регистъра на финансовите институции по чл. 3а от Закона за кредитните институции (ЗКИ) на БНБ, следователно дружеството, влиза в обхвата на задължените субекти по чл. 4, ал. 1 от ЗМИП. Със ЗМИП за определени правни субекти, за които се предвиждат задължения за предприемане на мерки за превенция, в частност - действия по идентифициране на клиенти и проверка на тяхната идентификация (чл. 3, ал. 1, т. 1 от ЗМИП).

В разпоредбите на глава V от ЗМИП, а именно в чл. 52 и чл. 53 е отразено, че Идентифицирането на клиентите и проверката на идентификацията се извършват чрез използване на документи, данни или информация от надежден и независим източник.

Определен е начинът на идентифицирането на клиентите и проверката на тяхната идентификация. За физическите лица се изисква представяне на официален документ за самоличност и регистриране на неговия вид, номер, издател, както и на името, адреса, единния граждански номер, а за физическите лица, имащи качеството на едноличен търговец - и чрез представяне на документите, идентифициращи го в търговското му качество. Съгласно чл. 53, ал. 1 от ЗМИП - Идентифицирането на физическите лица се извършва чрез представяне на официален документ за самоличност и снемане на копие от него.

Следователно служителите на финансовата институция снемат копие на личната карта при първоначалното посещение в небанковата финансова институция, след което, те трябва да сверяват истинността на предоставените от лицето данни, а не всеки път да снемат ново копие или да сканират отново личната карта.

Съгласно чл. 53, ал. 2 при идентифицирането на физически лица се събират данни за:

1. имената;

2. датата и мястото на раждане;

3. официален личен идентификационен номер или друг уникален елемент за установяване на самоличността, съдържащ се в официален документ за самоличност, чийто срок на валидност не е изтекъл и на който има снимка на клиента;

4. всяко гражданство, което лицето притежава;

5. държава на постоянно пребиваване и адрес (номер на пощенска кутия не е достатъчен).

При встъпване в делови взаимоотношения се събират и данни за професионалната дейност на лицето и целта и характера на участието на лицето в деловите взаимоотношения чрез използване на документи, данни или информация от надежден и независим източник, попълване на въпросник или по друг подходящ начин. Въз основа на оценката на риска по глава седма от Закона, а именно във връзка с изясняване на произхода на средствата лицата по чл. 4 може да събират допълнителни данни при условията и по реда на правилника за прилагане на закона. Когато в официалния документ за самоличност не се съдържат всички данни по ал. 2, събирането на липсващите данни се извършва чрез представяне на други официални документи за самоличност или други официални лични документи, чийто срок на валидност не е изтекъл и на които има снимка на клиента, и снемане на копие от тях. При липса на друга възможност събирането на данните по ал. 2, т. 3 и 5 може да се

извърши и чрез представянето на други официални документи или документи от надежден и независим източник. Когато идентифицирането се извършва без присъствието на подлежащото на идентификация физическо лице, идентифицирането може да се извърши и чрез представяне на копие на официален документ за самоличност. В тези случаи проверката на събраните идентификационни данни се извършва по реда на чл. 55, ал. 2.

Процедурата по идентифициране на клиента е задължителна за небанковите финансови институции. В чл. 2, ал. 1 от Правилника за прилагане на Закона за мерките срещу изпирането на пари е посочено, че това се извършва чрез представяне на официален документ за самоличност и снемане на копие от него, а в ал. 3 са изчерпателно изредени данните, които се събират:

1. имената;

2. датата и мястото на раждане;

3. официален личен идентификационен номер или друг уникален елемент за установяване на самоличността, съдържащ се в официален документ, чийто срок на валидност не е изтекъл и на който има снимка на клиента;

4. гражданство;

5. държава на постоянно пребиваване и адрес (номер на пощенска кутия не е достатъчен).

В глава III от ЗМИП са разписани сроковете на съхранение на информация и статистически данни. Разпоредбите на чл. чл. 67, ал. 1 гласи, че лицата по чл. 4 (в конкретния казус небанковите финансови институции) съхраняват за срок 5 години всички събрани и изготвени по реда на този закон и правилника за прилагането му документи, данни и информация.

В случаите на установяване на делови взаимоотношения с клиенти, както и в случаите на встъпване в кореспондентски отношения горецитираният срок започва да тече от началото на календарната година, следваща годината на прекратяването на отношенията.

Съгласно чл. 4, пар. 7 от Регламент (ЕС) 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните) „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. Като администратор на лични данни по смисъла на чл. 4, пар. 7 от Общия регламент, небанковата финансова институция („Б.Ф.“ ООД) има задължение да обработва личните данни на физическите лица в случаите, когато това е допустимо. Обработването на лични данни в конкретния случай отговаря на изискването на чл. 6, пар. 1, буква в) от Общия регламент относно защитата на данните, а именно **обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора.**

Обработването на лични данни от финансовата институция следва да се извършва при спазването на принципите изброени в глава II от Регламента, чл. 5 – личните данни да са: обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“); събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите“); подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“); точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“); съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“); обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба,

унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

Относно втория поставен в искането въпрос, а именно при установяване, че физическо лице е заявило и/или получило паричен заем по реда на Закона за предоставяне на финансови услуги от разстояние от небанкова финансова институция, чрез т.нар. „кражба на самоличност“, когато едно лице се представя за друго, задължена ли е небанковата финансова институция, като администратор на лични данни, да уведомява надзорния орган за нарушаване сигурността на личните данни съгласно изискванията на чл. 33 от Регламент (ЕС) 2016/679 (GDPR), то същото нарушение представлява риск за правата на физическите лица. чл. 33 от Общия регламент относно защитата на данните, следва да бъде разглеждан във връзка със съображение 85 от същия, а именно нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен начин, да доведе до физически, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица**. Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми надзорния орган за нарушението на сигурността на личните данни без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него**, освен ако администраторът не е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и че информацията може да се подаде поетапно без ненужно допълнително забавяне.

Във връзка с горното и на основание чл. 58, ал. 3 от Общия регламент за защита на данните, Комисията за защита на лични данни изрази следното

СТАНОВИЩЕ:

Небанковите финансови институции, като администратори на лични данни, са задължени при идентификация на клиента или проверките, да изискват официален

документ за самоличност, съдържащ снимката му, какъвто документ е лична карта, както и да направи копие от него и да го съхранява пет години (чл. 67, ал. 1 от ЗМИП). Задължението е съгласно чл. 53, ал. 1 от Закона за мерките срещу изпирането на пари, а именно идентифицирането на физическите лица се извършва чрез представяне на официален документ за самоличност и снемане на копие от него.

При установяване, че физическо лице е заявило и/или получило паричен заем по реда на Закона за предоставяне на финансови услуги от разстояние от небанкова финансова институция, чрез т.нар. „кражба на самоличност“, когато едно лице се представя за друго, задължение на небанковата финансова институция, като администратор на лични данни, да уведоми надзорния орган за нарушаване сигурността на личните данни съгласно изискванията на чл. 33 от Регламент (ЕС) 2016/679 (GOPR). Нарушението на сигурността на личните данни може да доведе до риск за правата и свободите на физическите лица, поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми надзорния орган за нарушението на сигурността на личните данни без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него (съображение 85 от Регламента). Задължение на администратора на лични данни е, също така да уведоми субекта на данните за нарушение на сигурността на личните му данни (съгласно разпоредбите на чл. 34 от Общия регламент).

ЧЛЕНОВЕ:

Цветелин Софрониев /п/

Мария Матева /п/

Веселин Целков /п/