

РЕШЕНИЕ
от 21.04.2010г.

Комисията за защита на личните данни (КЗЛД), в състав: председател Венета Шопова и членове : Красимир Димитров, Валентин Енев, Мария Матева и Веселин Целков, на редовно заседание, проведено на 21.04.2010 год. (Протокол № 14), разгледа молба, рег. № 5764/04.03.2010г. от „Ситибанк Н.А.-клон София” (клон на чуждестранен търговец), чрез пълномощника на управителите на клона Славена Атанасова, за издаване на разрешение от Комисията за предоставяне на лични данни от клона като администратор на лични данни на чуждестранно юридическо лице.

ФАКТИЧЕСКА ОБСТАНОВКА:

Съгласно искането получателят на данните ще бъде „Ситигруп Текнолъджи Инк.”-дружество, установено на територията на САЩ. Видно от информацията в молбата, трансферът на данни засяга служители, консултанти и изпълнители по договори, включително постоянен и временен персонал, нает на базата на договор за наемане на работа. Предмет на трансфер ще бъдат следните категории лични данни, засягащи посочените групи физически лица : социално осигуряване; номера на кредитни карти; номер на сметка; национален осигурителен номер; единен граждански номер ЕГН и IBAN (айбан) номер.

Целите, за които личните данни ще бъдат предоставяни са, както следва: наблюдение на определена група изходящи електронни писма, спазване на Политиката и Стандартите за информационна сигурност на Ситигруп, както и упражняване на различни форми на контрол. Указано е, че данните ще бъдат предадени в чужбина по електронен път, като защитата им ще се осъществява най-общо чрез защитна стена (Fire Wal), криптиране на лични данни за онлайн излъчване или транспортиране посредством носители на данни (ленти и модули или други носители), като всички транзакции ще протичат през глобален мрежов рутер на „Ситигруп”, който ще бъде защитен от Защитата на техническата инфраструктура на „Ситигруп”.

ПРАВЕН АНАЛИЗ:

При анализа на изложеното в искането, както и приложените към него документи, се установи следното:

„Ситибанк Н.А.-Клон София” е клон на чуждестранен търговец със седалище и адрес на управление: гр. София, общ. Столична, район Оборище , бул. “Княгиня Мария Луиза” 2, ет. 5 и с широк предмет на дейност, като публично привличане на влогове или други възстановими средства и предоставяне на кредит или друго финансиране за своя сметка и на собствен риск; извършване на услуги по парични преводи; издаване и администриране на други средства за плащане (платежни карти, пътнически чекове и кредитни писма); дейност като депозитарна или попечителска институция; финансов лизинг; гаранционни сделки; парично брокерство и други.

За осъществяване на предоставянето на данните в САЩ между износителя на данните „Ситибанк Н.А.-клон София” и вносителя на данните „Ситигруп Текнолъджи Инк.” е сключен договор за трансфер на данни с използване на общи договорни клаузи съгласно Решение 2002/16 от 27 декември 2001 година относно общите договорни клаузи за трансфера на лични данни към лицата, които ги обработват, установени в трети страни съгласно Директива 95/46/ЕО. Видно от този договор, вносителят на данните “Ситигруп Текнолъджи Инк.” се състои от няколко обособени технологични

звена и бизнес операции. Тези звена отговарят за предоставяне на поддръжка на системата (напр. Разрешаване на проблеми, технически въпроси) и управление на разработването на приложения и доработки, обхващащи целия жизнен цикъл – от концепцията и проекта до тестването и внедряването от потребителя. Екипите отговарят и за администриране на база данни, обновяване на системата, съхранение на данни на приложните сървъри в центъра за данни на „Ситигруп Текнолъджи Инк.“, както и поддръжка и тестване на непрекъсваемостта на бизнес операциите. Решаваща роля за осъществяването на тези дейности има Глобалният център за мониторинг на съдържание, който е в рамките на юридическото лице „Ситигруп Текнолъджи Инк.“. В тази връзка в искането за трансфер е посочено, че целта, за която ще бъдат трансферирани данните, е наблюдение на определена група изходящи електронни писма, спазване на Политиката и Стандартите за информационна сигурност на Ситигруп, упражняване на различни форми на контрол.

При извършената служебна справка в Регистъра на администраторите на лични данни и на водените от тях регистри, поддържан от КЗЛД, се установи, че дружеството е подало заявление за регистрация № 109 като администратор на лични данни и е вписано в регистъра с идентификационен номер 38. „Ситибанк Н.А.-клон София“ е заявило поддържането на 13 броя регистри. Трансферът на данни засяга информацията, поддържана в регистър „Мониторинг на съдържание“, обявен пред Комисията за защита на личните данни с актуализацията на администратора „Ситибанк Н.А.-клон София“ на 04.03.2010г. Необходимостта от трансфер на лични данни произтича от прилагането на т.нар. Програма за мониторинг на съдържание, която е в процес на внедряване в групата на „Ситигруп“. Целта на тази програма е да наблюдава ограничена група електронни писма. Програмата за мониторинг на съдържание наблюдава автоматично всички изходящи електронни писма, като електронни писма, изпратени от сметката за електронна поща на „Сити“ към сметка на „Сити“, която не е за електронна поща. Мониторингът открива наличието на определени видове идентифицираща личностна информация, които се изпращат некриптирани в нарушение на Стандартите за информационна сигурност на „Сити“. Програмата не наблюдава електронни писма, изпратени вътрешно между сметките за електронна поща на „Сити“ и не наблюдава входящите електронни писма (електронни писма, изпратени от сметка за електронна поща, която не е на „Сити“). Конкретните наблюдавани видове идентифицираща личностна информация се дефинират за всяка държава, в която е внедрена програмата Мониторинг на съдържание. Мониторингът на електронните писма се насочва от държавата по произход до сървъра за Мониторинг на съдържание, намиращ се в САЩ.

Програмата не пречи, нито блокира изпращането на електронни писма. Съответното електронно писмо, за което е установено, че съдържа идентифицираща личностна информация, отива до своята дестинация. Копие от него се изпраща до сървъра за управление на Мониторинга на съдържание за обработка и известяване на събитието на съответните страни. Всяка държава сама определя и поддържа прагове, свързани с броя и вида случаи на разкриване на идентифицираща личностна информация. В тази връзка се прилагат два подхода. При първия системата генерира уведомление до съответното отговорно лице и неговия ръководител, в което се съобщава, че е изпратено електронно писмо, което потенциално нарушава политиката за информационна сигурност на „Сити“. При втория се прави ръчен преглед на копие на електронното писмо преди изпращане на уведомление за нарушение на отговорния бизнес. Този преглед се извършва от Глобалния център за мониторинг на съдържание в

САЩ и копие на електронното писмо се съхранява в централната база данни. Това звено отговаря за ръчен преглед на определени електронни писма преди да бъде изпратено известие на отговорния бизнес за извършено нарушение. Целта на този преглед е да бъде отхвърлен всеки фалшив сигнал (електронни писма, обозначени с флаг от системата, без да е налице реално нарушение) и да класифицират нарушението като събитие на неизпълнение или като инцидент, свързан със сигурността.

Във връзка с реализирането на горепосочените дейности, от страна на „Ситибанк Н.А.-клон София” ще бъдат трансферирани лични данни от категориите физическа, социална и икономическа идентичност на служители, консултанти и изпълнители по договори, включително постоянен и временен персонал, нает на базата на договор за наемане на работа, както следва:

- социално осигуряване;
- номера на кредитни карти;
- номер на сметка;
- национален осигурителен номер;
- единен граждански номер;
- IBAN номер.

При извършената служебна проверка се установи, че посочените в регистър „Мониторинг на съдържание” лични данни съвпадат със заявените за трансфер. Предвидена е също така и възможността данните да бъдат предоставяни в трета държава-САЩ.

По отношение искането за трансфер на данни относно номера на кредитни карти следва да се има предвид, че става въпрос за платежен инструмент, който, съгласно чл.25, ал.3 от Наредба № 3 от 16 юли 2009г. за условията и реда за изпълнение на платежни операции и за използване на платежни инструменти, се използва само лично от оправомощения ползвател на платежни услуги. В указания 03-25009 на Българската народна банка - Номериране, дизайн, физически и технически спецификации на платежните карти - е посочено, че номерът на платежната карта, името на оправомощения ползвател и срока на валидност на картата задължително се записват върху лицевата страна на платежната карта (7.3). Поради това, че с изписването на номера на картата и името на картодържателя се постига еднозначна идентификация на оправомощения ползвател, информацията относно номера на дадена кредитна карта представлява лични данни от категорията икономическа идентичност. Евентуалното предоставяне на такива данни на трети лица не само представлява обработване на лични данни по смисъла на §1, т. 1 от Допълнителните разпоредби на Закона за защита на личните данни (ЗЗЛД), но би могло да застраши изпълнението на платежни операции чрез платежни карти. Предвид това предоставянето на информация относно номера на кредитни карти се явява прекомерно по отношение на целите, които си поставя “Ситибанк Н.А.-клон София” КЧТ с искането за трансфер на данни, а именно-наблюдение на определен група изходящи електронни писма, спазване на политиката и стандартите за информационна сигурност на “Ситигруп” и упражняване на различни форми на контрол. Изискванията за съотнесимост и съразмерност на обработването на личните данни по отношение на целите, за които се обработват, е основен принцип в областта на защитата на личните данни, установен в чл.2, ал.2, т.3 от ЗЗЛД и КЗЛД е длъжна да следи за спазването му.

Като приложение към договора са включени клаузи относно техническите и организационните мерки за сигурност, прилагани от вносителя на данните. Последният се задължава да осигури контрол на достъпа по начин, който да гарантира, че

неоправомощени лица няма да имат достъп до оборудването за обработка на данни, когато се обработват данните, трансферирани от износителя на данни. Вносителят се задължава също така да внедри подходящи мерки за предотвратяване на неоторизираното боравене с носители на данни, включително четене, копиране, поправка или премахване на носители на данни, съдържащи лични данни на клиентите на износителя. Въведени са и задължения за контрол върху паметта от данни и упражняване на контрол върху потребителя. Вносителят декларира, че лицата, които имат право да използват системата за обработка на данни на вносителя, имат достъп единствено до данните, които са в обхвата и степента на техните съответни разрешения за достъп. Разписани са и задължения във връзка с упражняването на контрол върху излъчването, въвеждането и транспортирането на данни.

Съгласно Директива № 95/46/ЕО на Европейския парламент и на Съвета трансфер на лични данни в трети страни може да бъде осъществен, само ако въпросната трета държава предоставя адекватно ниво на защита на данните.

Предоставянето на лични данни от администратор, установен на територията на Република България към друг администратор на лични данни извън страната, се извършва по реда на Закона за защита на личните данни, като определящ критерий относно режима на трансфер на данни е държавата, в която ще бъдат предоставени данните.

Предоставяне на лични данни в трета държава се допуска само, ако тя осигурява адекватно ниво на защита на личните данни на своя територия. Извършена бе служебна справка, от която се установи, че към настоящия момент получателят на данните не е включен в списъка на Сейф Харбар (Safe Harbour). В последния се включват дружества, които декларират пред Департамента по търговия на САЩ, че ще се придържат към така наречената Сейф Харбар рамка, създадена от Департамента по търговия в сътрудничество с Европейската комисия. Рамката Сейф Харбар съдържа насоки към дружествата, регистрирани в САЩ, за предоставяне на адекватно ниво на защита на личните данни, прехвърляни от страни – членки на Европейския съюз към тях.

На основание чл. 36а, ал. 4, т. 2 от ЗЗЛД КЗЛД не извършва преценка на адекватността на нивото на защита на личните данни в третата държава в случаите, когато е необходимо изпълнение на решение на Европейската комисия, с което тя се е произнесла, че определени стандартни договорни клаузи осигуряват адекватно ниво на защита. В конкретния случай износителят и вносителят на данните са използвали Решение 2002/16 от 27 декември 2001 година относно общите договорни клаузи за трансфера на лични данни към лицата, които ги обработват, установени в трети страни съгласно Директива 95/46/ЕО.

Предвид факта, че за извършване на трансфера се използват стандартни договорни клаузи съгласно горепосоченото решение на Европейската комисия и на основание чл.36а, ал.4, т.2 във връзка с ал.2 от ЗЗЛД Комисията за защита на личните данни

РЕШИ:

1. Разрешава на администратора на лични данни „Ситибанк Н.А.-клон София” да предостави лични данни от категориите физическа, социална и икономическа идентичност на физически лица (служители, консултанти и изпълнители по договори, включително постоянен и временен персонал) на дружество на територията на трета страна - „Ситигруп Текнолъджи Инк.”, САЩ за срока на Програмата за мониторинг на

съдържание, в следния обем: социално осигуряване; номер на сметка; национален осигурителен номер; единен граждански номер; IBAN номер.

2. Не разрешава на администратора на лични данни “Ситибанк Н.А.-клон София” да предостави информация относно номера на кредитни карти на физически лица (служители, консултанти и изпълнители по договори, включително постоянен и временен персонал) на дружество на територията на трета страна - „Ситигруп Текнолъджи Инк.”, САЩ.

Решението на Комисията може да се обжалва пред Върховния административен съд в 14 (четирнадесет) дневен срок от получаването му.

ПРЕДСЕДАТЕЛ:

Венета Шопова /п/

ЧЛЕНОВЕ:

Красимир Димитров /п/

Валентин Енев /п/

Мария Матева /п/

Веселин Целков /п/