Р Е Ш Е Н И Е
№ 467

гр. София, 27.01.2022 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 56 състав,** в публично заседание на 10.11.2021 г. в следния състав:

СЪДИЯ: Мария Ситнилска

при участието на секретаря Макрина Христова, като разгледа дело номер **6187** по описа за **2021** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по чл. 126 и сл. от Административно процесуалния кодекс (АПК) във връзка с чл. 38, ал. 6 от Закона за защита на личните данни (ЗЗЛД).

Образувано е по жалбата на [фирма], ЕИК[ЕИК], представлявано от изпълнителния директор В. Т. против решение № ППН-01-1903/2019 от 13.04.2021 г. на Комисията за защита на личните данни в частта, с която жалба № ППН-01-1903/23.12.2019 г., подадена от Н. Д. И. е обявена за основателна за нарушение на чл. 32, § 1, б. „б“ от Регламент /ЕС/ 2016/679 и в частта, с която на основание чл. 58, § 2, б. „и“ във връзка с чл. 83, § 4, б. „а“ от Регламент 2016/679 на оспорващото търговско дружество, в качеството му на администратор на лични данни, е наложено административно наказание „имуществена санкция“ в размер на 5000 лева. Изложени са доводи за незаконосъобразност на оспореното решение, поради противоречието му с материално правните разпоредби и несъответствие с целта на закона. Оспорва се изводът на административния орган, че дружеството не е предприело достатъчно технически и организационни мерки за защита на системата. В тази връзка се посочва, че дружеството прилага Политика за контрол на достъпа до системите на онлайн книжарницата на [фирма], като мерките са съобразени с изискванията на чл. 45 от ЗЗЛД, планират се към момента на определяне на средствата за обработване на лични данни и се прилагат при самото обработване на личните данни. Твърди се, че мерките включват свеждане на данните до минимум (не съхраняват банковите сметки на клиентите на интернет магазина), и въвеждане на необходимите гаранции в процеса

на обработване на лични данни. Излагат се доводи, че дружеството е предприело всички необходими мерки за предотвратяване на нерегламентиран достъп до разплащателната система на електронния си магазин, отчитайки качеството, тежестта и последиците, които биха могли да възникнат от нарушението на сигурността на данните. Посочва се, че в решението липсват мотиви защо Комисията счита, че не са предприети достатъчно технически и организационни мерки. В заключение се излагат съображения, че [фирма] не е извършило нарушение на сигурността на личните данни, тъй като дружеството не съхранява данни за банковите карти на клиентите, а те са извлечени по незаконен начин от трето лице през дублираща страница, имитираща системата на БОРИКА. Осъществен е нерегламентиран достъп до компютърно-информационни ресурси и промяна на компютърни данни, в резултат на което е настъпил инцидент, за който дружеството е уведомило компетентните правоохранителни органи и потенциално застрашените клиенти, с цел предотвратяване на вредните последици. Моли съда да постанови решение, с което да отмени решението в оспорените му части. Претендира разноски.

Ответникът - Комисията за защита на личните данни не изразява становище по жалбата.

Заинтересованата страна Н. Д. И. не изразява становище по жалбата.

Административен съд София-град, като взе предвид изложеното в жалбата и представените по делото писмени доказателства, прие за установено от фактическа страна следното:

Административното производство пред Комисията за защита на личните данни е образувано по жалба рег. № ППН-01-1903/23.12.2019 г., подадена от Н. Д. И. за нарушаване на ЗЗЛД. Конкретното нарушение е описано в жалбата по следния начин: на 02.11.2019 г., след направена поръчка към ciela.com и след заплащане с V. кредитна карта, поръчката не е завършена успешно и плащането не е отчетено, след което и до момента на депозиране на жалбата поръчката стой на сайта със статут „Прекъсната“. На 13.12.2019 г. Н. И. е получил обаждане от служител на [фирма], който му е съобщил, че е направено плащане преди минути с кредитната му карта и има съмнение, то е нерегламентирано. При проверка на електронната си поща Н. И. е попаднал на имейл от [фирма] от 05.12.2019 г., към който е прикрепено уведомително писмо изх. № 709/05.12.2019 г., в което се посочва, че е налице „съмнение за осъществен нерегламентиран външен достъп до администраторски профил в онлайн книжарница С. (https: ciela.com) и „възможно е трето неоторизирано лице да е извършило неправомерно извличане на информация: име и фамилия, имейл адрес, телефон, адрес, данни от банкова карта“.

Със съобщение № ППН-01-1903/2019#2 от 14.04.2020 г. [фирма] е уведомено за образуваното административно производство, като му е предоставена възможност да изрази становище и да представи доказателства. Търговското дружество се е възползвало от така предоставената му възможност, като е изразило писмено становище № ППН-01-1903/2019#3 от 29.04.2020 г., в което е изтъкнало, че подателят на жалбата е пренебрегнал уведомлението му от 05.12.2019 г., с което същото е изпълнило задължението си за уведомяване на субекта на данните по чл. 68, ал. 1 от ЗЗЛД. Изтъкнало е, че дружеството не съхранява данни за банковите карти на клиентите, както и че е изпълнило задължението си по чл. 33, ал. 1 от ОРДЗ и чл. 67, ал. 1 от ЗЗЛД да уведоми КЗЛД в срок от 72 часа за вероятност за извършено нарушение на сигурността на обработването на личните данни (уведомително писмо

изх. № 709/05.12.2019г.).
С Уведомление изх. № 704/04.12.2019 г. (вх. № ППН-02-64405.1.20219 г. на КЗЛД), на основание чл. 33, ал. 1 от Регламент (ЕС) 2016/679 [фирма] е уведомила КЗЛД за вероятност за извършено нарушение на сигурността на обработването на лични данни, като е предоставило дължимата се информация по чл. 67, ал. 3 от ЗЗЛД за възможно наличие на компютърна атака към сигурността, в резултат на която има съмнение за нарушаване на сигурността на данните. На 10.12.2019 г. е депозирано и второ Уведомление. Със заповед № РД-15-104 от 20.05.2020 г. на председателя на КЗЛД по повод постъпилото уведомление по чл. 33 от Регламент ЕС/ 2016/679 е назначена проверка на [фирма]. Резултатите от проверката са обективирани в Констативен протокол от 19.06.2020 г. По Уведомлението и по резултатите от проверката Комисията се е произнесла с решение по т. 2 по протокол №43/07.10.2020 г. С писмо изх. № ППН-02-644/19 #11 от 10.11.2020 г. КЗЛД е уведомила [фирма] за решението на Комисията според което, на основание чл. 57, § 1, б. „а“ във връзка с чл. 58, § 1 от Регламент (ЕС) 2016/679, администраторът своевременно е предприел всички необходими мерки за предотвратяване на нерегламентиран достъп до разплащателната система на електронния си магазин, отчитайки естеството, тежестта и последиците, които биха могли да възникнат от нарушението на сигурността на данните.
Комисията се е произнесла с нарочно решение, обективирано в протокол № 46 от заседание, проведено на 28.10.2020 г. за допустимост на жалбата, конституирала е страните и е определила дата за разглеждане на жалбата по същество.
На проведеното на 13.01.2021 г. заседание на Комисията жалбата на Н. Д. И. е разгледана по същество. На заседанието са присъствали трима от членовете на КЗЛД, които са гласували „за“ решението. Решението е обективирано в протокол № 1, т. I от дневния ред, т. 3. Същото е мотивирано с това, че [фирма] не е предприела достатъчно организационни и технически мерки, като е допуснала вграждането на зловреден код, който дава възможност за неправомерен достъп до лични данни на клиентите на електронния магазин на [фирма], включително имена, номер на банкови карти, тип банкова карта, номер на карта, валидност на карта и секретен код.
Въз основа на така проведеното административно производство, Комисията за защита на личните данни е издала решение № ППН-01-1903/2019 от 13.04.2021 г., с което на основание чл. 38, ал. 2 от ЗЗЛД е обявила жалбата на Н. Д. И. за основателната за нарушение на чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/679 и на основание чл. 58, § 2, б. „и“ във връзка с чл. 83, § 4, б. „а“ от Регламент (ЕС) 2016/679 на администратора [фирма] е наложено административно наказание – имуществена санкция в размер на 5000 лева. От фактическа страна констатацията за извършено нарушение на чл. 32, § 1, б.“б“ от Регламент (ЕС) 2016/679 е мотивирана с осъществен нерегламентиран достъп до компютърно-информационни ресурси и промяна на компютърни данни-въведен е компютърен код и компютърни данни в базата данни на ciela.com, като посредством това въвеждане на компютърен код към вече съществуващия код е извършено препращане към дублираща страница, имитираща системата БОРИКА, към която препраща модула за плащане на електронния магазин, и чрез която е събирана информация за клиентите, подали заявка за покупка чрез банкова карта в електронния магазин. Визираните факти са квалифицирани като бездействие на администратора на лични данни, изразяващо се в непредприемане на достатъчно технически и организационни мерки за защита на системата му, довело до достъп на

трето лице до нея и въвеждане на код, чрез който се препраща към имитираща система на БОРИКА, като по този начин клиентите на електронния магазин предоставят данните си на трето лице без право на достъп.
Въз основа на така установеното от фактическа страна настоящият съдебен състав обосновава следните правни изводи:
Жалбата е ПРОЦЕСУАЛНО ДОПУСТИМА, като подадена в срок, от легитимирано за това лице и срещу подлежащ на оспорване индивидуален административен акт. Съобщението за постановеното решение е получено на 26.04.2021 г., а жалбата е подадена до административния орган на 07.05.2021 г.
Разгледана по същество жалбата е ОСНОВАТЕЛНА по следните съображения:
Оспореното в настоящото производство решение е издадено от компетентен административен орган - Комисията за защита на личните данни, в съответствие с предоставените й правомощия по чл. 38, ал. 3 от ЗЗЛД, съгласно която разпоредба, при подадена до КЗЛД жалба от субектът на данни, който счита, че са нарушени правата му по Регламент (ЕС) 2016/679 и по ЗЗЛД, Комисията се произнася с решение, като може да приложи мерките по чл. 58, § 2, букви "а" - "з" и "й" от Регламент (ЕС) 2016/679 или по чл. 80, ал. 1, т. 3, 4 и 5 и в допълнение към тези мерки или вместо тях да наложи административно наказание в съответствие с чл. 83 от Регламент (ЕС) 2016/679, както и по глава девета. Т.е., доколкото Комисията е сезирана от лице, считащо, че са нарушени правата му по ЗЗЛД, като е осъществен неправомерен достъп до негови лични данни, то в нейните правомощия е да се произнесе с решение, което подлежи на оспорване на административния съд. На основание чл. 9, ал. 4 във връзка с ал. 3 от ЗЗЛД решенията на Комисията се вземат с мнозинство от общия брой на членовете й, който съгласно чл. 7, ал. 1 от ЗЗЛД и чл. 4, ал. 1 от Правилника е председател и 4-ма членове при проведено открито заседание. След като изрично не е посочен вида на мнозинството, се приема, че то е обикновено, а не квалифицирано. Правилата за кворума и мнозинството са изложени в чл. 8, ал. 6 и ал. 7 от ПДКЗЛДНА: заседанията на Комисията се провеждат, ако на тях присъстват най-малко трима от нейния състав. Комисията взема решения чрез явно гласуване с мнозинство от три гласа. На проведеното на 13.01.2021 г. заседание на КЗЛД, когато е взето оспореното в настоящото съдебно производство решение, са присъствали трима от членовете на Комисията. Решението е прието с мнозинство, като трите гласа са достатъчни по закон. Предвид това, настоящият съдебен състав намира, че актът е постановен от компетентен орган и не е налице отменителното основание по чл. 146, т. 1 от АПК.
Административният акт е издаден в изискуемата писмена форма и е обективиран като решение, съгласно изискването на закона. Решението съдържа всички изискуеми реквизити, предвидени в чл. 59, ал. 2 от АПК, включително фактическите и правни основания за негово издаване. Налице е обаче противоречие в изложените мотиви, което разколебава решението на административния орган, обективирано в разпоредителната част на оспорения административен акт, за извършено нарушение на чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/679. Констатира се противоречие между диспозитива на решението и мотивите, в частта им в която е посочено, че е извършена проверка, резултатите от която са обективирани в Констативен протокол от 19.06.2020 г., и за които резултати администраторът е уведомен с писмо изх. № ППН-02-644/19 #11 от 10.11.2020 г.. Става дума за решението на КЗЛД, взето на основание чл. 57, § 1, б. „а“ във връзка с чл. 58, § 1 от Регламент ЕС 2016/679, според което

администраторът своевременно е предприел всички необходими мерки за предотвратяване на нерегламентиран достъп до разплащателната система на електронния си магазин, отчитайки естеството, тежестта и последиците, които биха могли да възникнат от нарушението на сигурността на данните и последиците, които биха могли да възникнат от нарушението на сигурността на данните. От своя страна, така изложените мотиви противоречат на мотивите, че администраторът на лични данни не е предприел достатъчно технически и организационни мерки за защита на системата му, довело до достъп на трето лице до нея и въвеждане на код, чрез който се препраща към имитираща система на БОРИКА, като по този начин клиентите на електронния магазин предоставят данните си на трето лице без право на достъп.

В хода на административното производство не са допуснати съществени нарушения на процесуалните правила. Решението е постановено след като е дадена възможност на страните да изразят становище и представят писмени доказателства (чл. 36 от АПК във връзка с чл. 38, ал. 2 от Правилника), както и след разглеждане на жалбата по същество в открито заседание, съгласно чл. 40, ал. 1 от Правилника за дейността на Комисията за защита на личните данни и нейната администрация.

Констатираното противоречие в мотивите на оспореното решение от своя страна е довело до неправилно прилагане на материално правните разпоредби и противоречие с целта на закона.

Определението на понятието „лични данни“ се съдържа в чл. 4, § 1, т. 1 от Регламент (ЕС) 2016/679. Според чл. 4, § 2 от Регламент ЕС 2016/679 „обработване на лични данни“ е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

По делото не е спорно, че посредством въвеждането на компютърен код към вече съществуващия код на интернет магазина на [фирма], трети лица са получили достъп до данни на клиентите му в обем: име и фамилия, адрес, номер на банкова карта, които представляват лични данни по смисъла на по чл. 4, § 1, т. 1 от Регламент /ЕС/ 2016/679, като информация, отнасяща се до физическо лице, която дава възможност то да бъде идентифицирано с тези специфични признаци.

В разпоредбата на чл. 4, т. 7 от Регламент (ЕС) 2016/679 се определя, че администратор на лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с друг определя целите и средствата за обработване на лични данни, когато целите и средствата за това обработване се определя от правото на съюза или правото на държавата членка. В т. 8 от Регламента е записана и дефиницията на „обработващ лични данни“, а именно: „физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора“. В този смисъл, за да носи отговорност едно лице за обработване на личните данни на друго лице в нарушение на ЗЗЛД и Регламент (ЕС) 2016/679, то лицето използващо неправомерно данните следва да има качеството „администратор“ или „обработващ лични данни“. По делото не е спорно, че [фирма] е администратор на лични данни.

Спорът по делото е правени и се изразява в това дали оспорващият е осъществил състава на вмененото му нарушение по чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/ 679.

Съгласно визираната разпоредба, като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно: б/ способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване.

Обратно на възприетата от ответната страна теза, описаната в мотивната част на решението фактическа обстановка не презюмира противоправно поведение на [фирма], като администратор на лични данни, изразяващо се в бездействие на последния да приложи подходящи технически и организационни мерки за осигуряване защитата на базата данни така, че срещу нея по никакъв начин, от никого и с никакви средства да не може да бъде достъпено. Възприемането на тази теза би означавало, че всеки, който е станал обект на каквото и да било посегателство, следва да понесе отговорност, че е допуснал извършването на същото, тъй като не е положил достатъчно грижи за предотвратяването му. От една страна, ответникът вменява в тежест на оспорващия това нарушение, но от друга страна, в свое нарочно решение по т. 2 по протокол №43/07.10.2020 г. Комисията приема, че на основание чл. 57, § 1, б. „а“ във връзка с чл. 58, § 1 от Регламент (ЕС) 2016/679, администраторът своевременно е предприел всички необходими мерки за предотвратяване на нерегламентиран достъп до разплащателната система на електронния си магазин, отчитайки естеството, тежестта и последиците, които биха могли да възникнат от нарушението на сигурността на данните. В тази връзка следва да се отбележи липсата на установяване от страна на административния орган какви точно технически и организационни мерки е следвало да предприеме администратора на лични данни в конкретния случай. Във фактическите установяване на КЗЛД изцяло липсват обективните признаци на нарушението. Общият бланкетен израз „администраторът на лични данни не е предприел достатъчно технически и организационни мерки за защита на системата му“ не обосновава извършено нарушение и реализиране на санкционна отговорност. В хода на производство е останало неизяснено какво точно е следвало да предприеме [фирма], за да не допусне въвеждането на допълнителен код с системата си за електронна търговия. Безспорно, това въвеждане на допълнителен код и допълнителна информация и създаването на дублираща БОРИКА разплащателна система, представлява хакерска атака от неизвестни лица-физически извършители, чиито действия не могат да се вменят в тежест на търговското дружество. В тази връзка следва да се

отбележи, че именно в резултат на тези злонамерени постъпки, дружеството е инициирало нарочна проверка, при която се разкрива извършеното неправомерно обработване на личните данни от трето лице. Именно, администраторът на лични данни е този, който сигнализира правоохранителните органи за извършената атака на интернет книжарницата. Предвид конкретиката на случа, че неправомерното обработване на лични данни е осъществено от трето лице чрез компютърно престъпление, ангажирането на отговорността на [фирма] се явява априори, без оглед на неизпълнение на негови конкретни задължения. Това ангажиране на отговорността противоречи на принципа за законоустановеност на нарушението и наказанието. Изложеното обосновава извод за издаване на оспореното решение в противоречие с материално правните норми и на основание чл. 146, т. 4 от АПК е основание за неговата отмяна.

Предвид изхода на спора на основание чл. 143, ал. 1 от АПК искането на оспорващия за присъждане на разноски следва да бъде уважено.

С оглед на изложеното и на основание чл. 172, ал. 2 от АПК, Административен съд София- град, Второ отделение, 56-ти състав

Р Е Ш И:

ОТМЕНЯ по жалбата на [фирма], ЕИК[ЕИК], представлявано от изпълнителния директор В. Т. решение № ППН-01-1903/2019 от 13.04.2021 г. на Комисията за защита на личните данни в частта му по т. 1, с която жалба № ППН-01-1903/23.12.2019 г., подадена от Н. Д. И. е обявена за основателна за нарушение на чл. 32, § 1, б. „б“ от Регламент /ЕС/ 2016/679 и в частта му п т. 2, с която на основание чл. 58, § 2, б. „и“ във връзка с чл. 83, § 4, б. „а“ от Регламент 2016/679 на оспорващото търговско дружество в качеството му на администратор на лични данни е наложено административно наказание „имуществена санкция“ в размер на 5000 лева.

ОСЪЖДА Комисията за защита на личните данни да заплати на [фирма], ЕИК[ЕИК], представлявано от изпълнителния директор В. Т. разноски по делото в размер на 50 (петдесет) лева.

Решението подлежи на обжалване в 14-дневен срок от съобщаването му пред Върховния административен съд.

СЪДИЯ: