Протокол
№

гр. София, 04.01.2022 г.

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 23 състав,**
в публично заседание на 04.01.2022 г. в следния състав:
СЪДИЯ: Антоанета Аргирова

при участието на секретаря Емилия Митова, като разгледа дело номер **10477** по описа за **2019** година докладвано от съдията, и за да се произнесе взе предвид следното:

4

След спазване на разпоредбите на чл. 142, ал. 1 от ГПК, във връзка с чл. 144 от АПК, на именното повикване в 13:00 ч. се явиха:

ЖАЛБОПОДАТЕЛЯТ: НАЦИОНАЛНА А. ПО ПРИХОДИТЕ - редовно уведомен, представлява се от главен юрисконсулт А. и юрк. М., с пълномощно по делото.
ОТВЕТНИКЪТ: КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ - редовно уведомен, се представлява от юрк. П., с пълномощно по делото.
Софийска градска прокуратура: редовно уведомена, не изпраща прокурор за участие в производството по делото.
Вещото лице: А. Н. К. - редовно призован, се явява.

Процесуалните представители на страните (поотделно): Да се даде ход на делото.

СЪДЪТ, като съобрази липсата на процесуални пречки за разглеждане на делото в днешното съдебно заседание,

ОПРЕДЕЛИ:

ДАВА ХОД НА ДЕЛОТО.
Предвид депозирането на заключение в предходното съдебно заседание, съдът намира, че не са налице пречки за изслушване на вещото лице, поради което снема самоличност на вещото лице.
А. Н. К. – 50г., българин, български гражданин, неосъждан, без дела със страните.
Предупреден за наказателната отговорност по чл. 291 от НК.

Обеща да даде вярно и безпристрастно заключение.
Вещото лице: Депозирал съм писмено заключение в срок, което поддържам.
ЮРК. М.: Нямам въпроси към вещото лице.

На въпроси на съда:
Вещото лице: Аз съм изследвал документите, които са приложени по делото и лог-файловете, които са на място. Различните документи и файлове са за различни периоди. Не мога да направя категоричен извод за периода преди юли 2019г. Няма как да се установи към момента на теча на лични данни дали тези мерки, посочени в задача №2 от заключението са били взети. Съдът е приел, че течът на лични данни е от момента на неговото публично узнаване, но в технологичен аспект не е сигурно кога точно е станало реално това. Много вероятно е да е станало по-рано и на няколко пъти. Въз основа на моя опит, мога да обобщя: В различни периоди НАП е създала много документи с различни инструкции и правила касаещи личните данни, но те не са обединени и структурирани в единна политика или единен йерархичен документ. Това създава проблеми при ползването. Второто нещо, което констатирах, че липсва и личната отговорност на служителите. Има създадени правила, има създадени изисквания, но няма лична отговорност на служителите, ако те не ги спазват. Липсват обучения за защита на личните данни на целия състав от служители. Имам предвид обучения, които са предназначени за работещите в НАП. Единственият договор, който е приложен по делото, описан в последната точка от заключението ми, е с Информационно обслужване и субект, наречен Лаборатория за киберсигурност. Този договор включва много точки, една от които е обучението за сигурност на данните, но то касае само малка група от служители на НАП, т.е. касае се за частично обучение. Аз не съм сигурен в компетентността на Лабораторията по киберсигурност и Информационно обслужване-относно техните знания и технически възможности за сигурност на данните. Едновременно с това НАП за предходния и за същия период-2019 година имат и други договори с Информационно обслужване, които касаят аспекти на сигурността на компютърните системи в НАП. Според мен като вещо лице не е редно в чисто технически аспект едни и същи лица да бъдат ангажирани в процесите по инсталиране, експлоатация и обучение. Имам предвид, че при инсталирането на компютърни системи на НАП там се конфигурира сигурността в технически аспект. Според мен не е редно технически, защото се изкривява процеса едни и същи специалисти да извършват и инсталирането, и конфигурирането, и след това обучението на служителите, защото те представят едни и същи практики и по тази причина е препоръчително да има независим одит. В Банките, което е прието в цял свят, независими одитори проверяват какво самата банка е закупила, инсталирала и как са обучени нейните служители. Независими одитори, тъй като те не зависят от дейността на Банката, включително и от този, който е инсталирал технически съответния продукт,поради което имат най-голяма възможност за обективен контрол.
На въпрос на юрк. А.,вещото лице отговори:
Запознат съм с Инструкция №2, четох я във връзка с делото. Тази инструкция е подзаконов акт, който касае различни дейности в НАП, но не съдържа детайлни указания за всички дейности, които са необходими във връзка със сигурността на данни.
ЮРК. П.: Към кой момент тези три софтуера посочени на стр. 7 от заключението Ви са придобити от НАП, и имали указания или някакви вътрешни правила и кога следва

същите да бъдат въведени в експлоатация, и по-конкретно към теча на лични данни юли 2019 били ли са налични за въвеждане в експлоатация?
Вещото лице: При посещението ми в НАП, като първия път беше в началото на 2020 г., посочените софтуери бяха в процес на инсталиране, но няма данни кога са придобити от НАП. В НАП процесът по придобиване и инсталиране е доста дълъг, защото първо се инсталират в тестова среда, правят се обучения на администратори и чак впоследствие се инсталират в работна среда.
ЮРК. П.: Л.- файловете /технически дневници/ дали са налични към юли месец 2019г.?
Вещото лице: При извършване на изследването ми в НАП установих два вида технически дневници. Едните от тях касаят базите данни, те са описани на стр.8, стр.9 и стр.10 от заключението. Установени са файлове от 2019 г. от датата на узнаването на теча. Установих файлове, които са от юни месец 2019 г. и впоследствие от месец юли и месец август 2019 г. Тези файлове касаят технически обръщения, техническа комуникация с базите данни, те не касаят потребителите. На техническо ниво, базата данни е това, което съдържа информацията от системите на НАП, това е основният елемент от тяхната информационна система. НАП притежава няколко сървъра на база данни. Аз получих достъп до файловете, до тези лог- файлове на сървъра, от който вероятно са изтекли данните. Съществуват лог-файлове за периода от юни 2019 г. до момента на изследването извършено от мен, като те са много подробни. В тях има много техническа информация и затова не съм ги изследвал подробно. Допълнително при посещението ми в НАП изследвах системата за контрол на потребителите, включително и привилегированите потребители, в която също има данни към 15.07.2019 г., но тогава системата е работила в непълен капацитет, тъй като тя е била все още тестова. НАП са предприели множество мерки, но не са изискали помощ от компетентни органи за да определят дали нивото на мерките е достатъчно, както и нямат независим одит, каквито са добрите практики в Европейския съюз. Ако тези практики бяха използвани със сигурност защитата щеше да е на доста по-високо ниво. Запознат съм с одитите, които са правени от Държавна агенция електронно управление, макар и не в детайли. ДАЕУ не са независим одитор, не са известни техните технически компетенции в областта на сигурността на личните данни. От 20 години се занимавам с дейност по изследване на инциденти, настъпили вследствие на вирус или хакерски атаки. От 10 години ръководя лабораторията на У.. Моят експертен опит ми позволява да направя извод, че в НАП са липсвали конкретни адекватни мерки. Ще дам пример с банките: Всички банки по света, независимо в коя държава се намират, за да могат да приемат разплащане с дебитни и кредитни карти са длъжни да изпълняват стандарт, който са нарича „P. D.“, той е единен за цял свят, за всички банки. Това е много прагматичен стандарт и той забранява използването на софтуери, които не са проверени от независими лаборатории. Също така стандартът изисква всяка организация да има подробна методика за служителите, какво трябва да правят и съответно какво не трябва да правят. Банките подлежат на големи глоби, ако не спазват този стандарт. С. на НАП, кой независим одитор или друг одитор ги е проверил за сигурност. Положени са много усилия и са вложени много средства, но просто не са адекватните.

СЪДЪТ ПРИЕМА заключението по допусната СТЕ.
На ВЛ да се изплати възнаграждение в размер на 600 лв., за което се издаде РКО.

ЮРК А. И ЮРК М.: Няма да сочим и да представяме други доказателства
ЮРК. П.: Няма да соча и да представям други доказателства.

Съдът, като съобрази обстоятелството, че страните не сочат и не представят други доказателства за изясняване на спора от фактическа страна, както и че не се налага служебното събиране на такива,

ОПРЕДЕЛИ:

ПРИКЛЮЧВА събирането на доказателства.
ДАВА ХОД НА УСТНИТЕ СЪСТЕЗАНИЯ.

ЮРК. А.: Моля да постановите решение, с което да отхвърлите жалбата. Моля да не кредитирате заключението на вещото лице по съображения, които сме изложили в писмено становище, което представям. Искам да добавя във връзка със заявеното от вещото лице при изслушването му: Първо по отношение на Инструкция №2/08.05.2019 г., заявявам, че това е основен документ, който регламентира обработването на лични данни. Той не е единственият документ, тъй като функциите на НАП са изключително широки и затова има разработени още над 300 вида процедури, съобразно отделните функционалности. В тези процедури се говори общо за обработване на защитена информация, тъй като в НАП се обработват не само лични данни. Има и друга чувствителна информация, каквато например е осигурителната информация. Искам да кажа, че всеки служител попълва декларация и носи дисциплинарна отговорност. Всеки служител задължително преминава през едно общо обучение, включително и по отношение на обработването на личните данни. По тези съображения и като съобразите нашето писмено становище, депозирано днес, моля да не кредитирате заключението на вещото лице в частите, които сме посочили в становището. Моля да постановите решение, с което да уважите жалбата ни и да отмените оспореното решение на КЗЛД. Моля да присъдите юрисконсултско възнаграждение в полза на НАП.
ЮРК. П.: Считам издаденото решение на КЗЛД за правилно и законосъобразно, като кредитирам изцяло експертизата на вещото лице, която доказа в пълнота фактите, които са установени при проверката на КЗЛД, а имено, че към момента на теча на личните данни липсват лог-файлове, от които да се установи по какъв начин, от кого точно е извършен достъпа, съответно как е установено изтичането на данни на 6 000 000 български граждани. Факт е, че към момента на извършване на проверката, както и при изследването от вещото лице, операционната система О. 11.2.0.2 е била в остаряла версия и е актуализирана едва след извършване на проверката от КЗЛД. Всички представени документи от НАП по време на проверката са утвърдени със заповед преди 2018 г., т.е. НАП не е предприела никакви технически и организационни мерки след приемането на Регламента през 2016г. и дадения двегодишен гратисен период до влизането му в сила през 2018 г. за въвеждане на нормите на регламента да актуализира вътрешните си правила по отношение на обработката на личите данни, поради което според нас е възникнал огромният теч на лични данни на български граждани. В тази връзка моля съдът да потвърди решението в неговата цялост. Заявявам искане за присъждане на юрисконсултско възнаграждение.
ЮРК. М.: Моля за срок за писмени бележки.

СЪДЪТ ПРЕДОСТАВЯ на страните 7-дневен срок считано от днес за депозиране на писмени бележки по предмета на делото.

СЪДЪТ ОБЯВИ, ЧЕ ЩЕ СЕ ПРОИЗНЕСЕ С РЕШЕНИЕ В СРОК.

Протоколът е изготвен в съдебно заседание, което приключи в 13:58 часа.

СЪДИЯ:

СЕКРЕТАР: