Р Е Ш Е Н И Е
№ 4534

гр. София, 04.07.2022 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 23 състав,** в публично заседание на 30.05.2022 г. в следния състав:

СЪДИЯ: Антоанета Аргирова

при участието на секретаря Емилия Митова и при участието на прокурора Ива Цанова, като разгледа дело номер **5183** по описа за **2021** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е исково и е по реда на чл.226 и сл. АПК, вр.чл.203 и сл. АПК.

С Решение №4643/18.08.2020 година, постановено по адм.дело №11304/2019 година по описа на Административен съд София- град, АССГ, Второ отделение, 53 състав е отхвърлил иска с правно основание чл.1, ал.1 ЗОДОВ, предявен от М. К. С. срещу Национална агенция по приходите за осъждане на ответника да заплати на ищеца сумата от 1 000 лв., представляваща обезщетение за претърпени неимуществени вреди, вследствие на незаконосъобразно бездействие от страна на ответника, за периода от 15.07.2019 г. до настоящия момент, изразяващо се в неизпълнение в достатъчна степен на задължение по чл. 59, ал.1 ЗЗЛД и по чл. 24 и чл. 32 от Общия регламент относно защитата на лични данни ЕС 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. /GDPR/, а именно да гарантира достатъчно ниво на сигурност на обработваните от него лични данни на ищеца, довело до неразрешено разкриване или достъп до личните данни на ищеца, ведно със законната лихва върху тази сума, считано от 15.07.2019 г., алтернативно от датата на подаване на исковата молба, до окончателното изплащане на сумата.

С Решение №6083/19.05.2021 година, постановено по адм.дело №11509/2020 година по описа на Върховния административен съд, ВАС-Трето отделение е отменил първоинстанционното съдебно решение на АССГ и е върнал делото за ново разглеждане от друг състав. Задължителните указания /чл.224 АПК/, дадени с отменителното решение, са по приложението на процесуалния закон: При новото

разглеждане в подробен доклад по делото съдът да посочи относимите към спора факти, като разграничи спорните от безспорните. След определяне на спорните факти, на страните да бъдат дадени подробни указания по тежестта на доказване, съобразени с техните конкретни твърдения и с нормата на чл.82, §3 от Регламента, включително, но не изчерпателно, за необходимостта от специалния знания за изясняване на въпросите при какви конкретни обстоятелства е допуснато изтичането на данни, има ли нерегламентиран достъп, по какъв технически начин е осъществен и до какви конкретно устройства или системи, съхраняващи данни, изцяло на външна намеса ли се дължи достъпът и възможно ли е той да се дължи изцяло на външна намеса, какви технически мерки са предприети, за да предотвратят достъпа, достатъчни ли са те, предвид достиженията на техническия прогрес и различните рискове, технически възможно ли е било предотвратяването на изтичането на данни.
В съдебно заседание пред АССГ при новото разглеждане на делото, ищцата моли за уважаването на иска и за присъждането на разноските, направени до този момент.
Ответникът-Национална агенция по приходите се представлява от юрк.Т., който моли искът да бъде отхвърлен. Заявява искане за присъждане на юрисконсултско възнаграждение.
Участващият по делото прокурор от Софийска градска прокуратура дава заключение за недоказаност на предявения иск.
Административен съд-София град, след като обсъди доводите на страните, вкл.и като и прецени събраните при новото разглеждане на делото доказателства, в изпълнение на задължителните указания на ВАС по приложението на процесуалния закон, намира за установено следното:
От фактическа страна:
Ответникът НАП е специализиран държавен орган към министъра на финансите за установяване, обезпечаване и събиране на публични вземания и определени със закон частни държавни вземания /чл.2, ал.1 от ЗНАП/ и администратор на лични данни по смисъла на чл.4, т.7 от Общия регламент относно защитата на личните данни.
Страните не спорят от фактическа страна, че поради нерегламентиран достъп на неизвестно лице, публично оповестен на 15.07.2019 г., е изтекла информация от информационните масиви на НАП, съдържаща лични данни на общо 6 074 140 физически лица, от които 4 104 786 живи физически лица, български и чужди граждани, и 1 989 598 починали физически лица.
Ноторно известен е фактът, че след изтичането на лични данни от информационните масиви на НАП, последната е информирала за това С. градска прокуратура и Комисията за защита на личните данни.
По делото се представи и прие извадка от получен SMS, с посочен в него час-16.37 ч, но без посочена дата, със следното съдържание: „НАП: По заявка номер 4038 ИМА неправомерно разкрити лични данни“. Не е посочен телефонният номер, на който е получен SMS. Макар и тези данни да са непълни, съпоставени с липсата на оспорване от страна на ответника, че сред изтеклата информация са и лични данни на ищцата, съдът приема този факт за установен.
Със Заповед № ЗЦУ-746/25.05.2018 г. на изпълнителния директор на НАП е утвърдена политика по защита на личните данни в НАП. Утвърдена е Политика по информационна сигурност на НАП, версия 3.0 от м. май 2016 г. Утвърдена е Инструкция № 2/08.05.2019 г. за мерките и средствата за защита на личните данни, обработвани в НАП и реда за движение на преписки и заявяване на регистри. Като

приложение № 1, към чл. 24, ал.2 от Инструкцията, служителите на НАП попълват декларация за това, че ще пазят в тайна личните данни на трети лица, станали им известни при изпълнение на служебните им задължения, няма да ги разпространяват и да ги използват за други цели, освен за прякото изпълнение на служебните им задължения. Със Заповед № ЗЦУ-586/30.04.2014 г. на изпълнителния директор на НАП е наредено да се внедри С. по стандарт БДС ISO/IEC 27001:2006 в НАП. В НАП е изработена Методика за оценка на риска, версия 1.1 ноември 2015 г.

Със Заповед № ЗЦУ- 1436/15.10.2018 г. на изпълнителния директор на НАП са утвърдени „Указания за разработване, попълване и/или зареждане с данни на образци на документи и приложения, утвърдени на основание чл.10, ал.1, т.5 и т.7 от ЗНАП“, „Указания за обозначаване и работа с информация“, „Указания за попълване на образци на процедура“, „Указания за попълване на образеца на инструкция“ и други.

Видно от предоставена от Комисията за защита на личните данни / КЗЛД/ с нейно писмо изх.№ППН-02-33/2019 г.#151 от 29.07.2020 г. информация, пред КЗЛД като постоянно действащ независим надзорен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент (ЕС) 2016/679 и на ЗЗЛД /чл.61 ал.1 ЗЗЛД/, не е налице висящо или приключило производство, инициирано от ищцата.

От събраните по делото гласни доказателства чрез разпит на св.Е. М. се установяват негативните изживявания на ищцата във връзка с неправомерно разкритите й лични данни, които са продължили 2-3 месеца. Обстоятелството, че свидетелката е сестра на ищцата не е достатъчно за некредитиране на показанията. Нормално и житейски обосновано и негативните изживявания и емоции да бъдат споделени от ищцата с близък за нея човек. По делото не са налице данни, които да компрометират достоверността на дадените показания.

Вследствие разпределената между страните доказателствена тежест в изпълнение указанията на ВАС, направеното с определението от з.з. на 02.06.21 година, по искане на ответника е допусната и извършена съдебно-техническа експертиза. Видно от приетото по нея и неоспорено от страните заключение, изтичането на лични данни от сървъри на НАП е установено от НАП на 15.07.2019 г. след публикации в медиите, а реално кога е било осъществено не може да се установи еднозначно. Източването на целия обем от 10.7 Gb данни едва ли е осъществено еднократно, а най- вероятно се е случвало в продължителен период от врем, каквато е честата практика на хакерите, с цел да не натоварват излишно засегнатите системи, при което могат да бъдат евентуално открити. Използвана е атака от тип „S. injectoin“ срещу едно от програмните приложения на сайта на НАП - “VAT refund“, като чрез този тип атака, атакуващият се възползва от уязвимост в изходния код на конкретното уеб приложение и получава директен достъп до базата данни, което приложението използва, като предоставя административните данни за достъп до базата данни.

Всеки достъп до данни в информационни системи, по начин различен от предварително дефинираните администратори и/или потребители от страна на собственика на информационната система, следва да се разглежда като нерегламентиран. В конкретния случай чрез атака от тип „S. injectoin“срещу едно от програмните приложения на сайта на НАП - “VAT refund“ е получен нерегламентиран достъп до данните на 6 074 140 физически лица, с активна регистрация - 4 104 786 души, от които 24 507 чужденци и 4 057 328 души с активна регистрация и валидно

ЕГН.
Системите, от които е извършено източване на данни, са сървъри с операционна система W. server 2008R2 и база данни O. 11.2.02. O. неоторизиран достъп е засегнал всички бази данни на O. сървъра, към който има връзка уеб приложението "VAT refund".
Използваната в случая атака от тип „S. injectoin" не предполага необходимост от вътрешна намеса. За извършване на нерегламентирания достъп се използват публично достъпните функции на приложение или страница, като чрез него се подава специална команда, връщаща административните данни за достъп до базата данни. След получаването на тези данни, атакуващият се свързва директно към съответната База Данни и получава достъп до наличната информация в нея. В конкретния случай действията се дължат изцяло на външна намеса.
Когато се говори за осигуряване на защита на информацията, според ВЛ, не следва да се извършва позоваване единствено на техническите мерки, а следва да бъдат разглеждани комплексно с предприетите организационни такива. Всяка организация е необходимо да изгради собствена С., включваща политики, правила и конкретни инструкции за осигуряване на Информационната сигурност, базирано на Оценка на риска, направена на базата на конкретните процеси и информационни активи. Една такава С. следва да бъде непрекъснато обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност. Към момента на теча, НАП е бил разработила, внедрила и използвала С., изградена на основни правила, базирани на стандарта за информационна сигурност БДС 180/1ЕС 27001/2006 и в последствие актуализирана към по- новата версия БДС 180/1ЕС 27001/2014.
На база на тази С. са били определени и изпълнени преценените към онзи момент необходими и достатъчни технически и организационни мерки за защита на информацията, но явно е пропуснато да бъде тествано конкретното приложение за атаки от типа на „S. injectoin" при въвеждането му в експлоатация, както и не е бил извършван последващ контрол на сигурността на засегнатото W. приложение.
Непосредствено след установяване на теча на данни, от страна на НАП са предприети незабавни коригиращи действия в наличните им технически и организационни мерки за защита на информацията, включващи:Създаден съвместен екип от експерти на НАП, ДАНС, ГДБОП и ДА „Електронно управление" за установяване на причините за извършения нерегламентиран достъп до базите данни на НАП; Извършена е промяна/нулиране на паролите на потребителите за достъп до приложения и други активи.
Преустановена е работата на следните приложни системи на НАП, по препоръка на представители на ДАНС и ГДБОП и след преглед от НАП: Система за възстановяване на ДДС от друга държава членка на "VAT refund"; Бюлетин на издирваните от НАП лица (чл.32 от ДОПК/; Публичен бюлетин по чл.182, ал.3, т.2 във връзка с §5, ал.3 от ДОПК - два списъка; Публично достъпните услуги за регистрация на S. карти и подаване на данни от ФУ/ИАСУТД към НАП /услугите, достъпни през мрежите на мобилни оператори са вече активни и работещи, Публично достъпните приложения за тестване на ФУ/ИАСУТД от Български институт по метрология и фирми /приложенията за тестване от БИМ са достъпни от 26.7.2019 г. от БИМ през нарочно изграден за целта защитен канал vpn/; -Публично достъпната услуга за регистрация и подаване на данни от организатори на хазартни игри от разстояние към НАП; Публично достъпните приложения за тестване на подаването на данни от

организатори на хазартни игри от разстояние от Български институт по метрология {приложенията за тестване от БИМ са достъпни от 26.7.2019 г. от БИМ през нарочно изграден за целта защитен канал урп); Регистрацията на лица за извършване на резервации в почивните бази на НАП

Възложен е и е извършен е пълен технически одит по сигурността от външен изпълнител, включващ преглед, анализ и препоръки за корекции на информационните системи на НАП и комуникационни и инфраструктурни елементи, с приоритет на достъпните извън вътрешната мрежа на НАП, за уязвимости.

Извършена е корекция на програмните приложения, достъпни извън вътрешната мрежа на НАП, съгласно направени препоръки от представителите на ДАНС - поставяне на captcha защита.

Изготвено е описание на неправомерно публикуваната информация на високо и по-детайлно ниво.

Извършен е анализ на информацията, която неправомерно е публикувана, за наличие на идентификатори на физически лица с активна регистрация в регистъра на задължени лица в НАП с оглед изпълнение на задълженията по ЗЗЛД. Установено е наличието на 4 057 328 лица с ЕГН, 24 507 лица с ЛНЧ и 23 085 лица с сл.№ на НАП с активна регистрация.

Разработено е и публикувано на 25.7.2019 г. за реално ползване на web-базирано приложение, достъпно през Интернет страницата на НАП за проверка на нарушена сигурността на личните данни, вследствие на осъществен неправомерен външен достъп до данни на Национална агенция за приходите.

Въз основа на Доклада за дейността на Временната анкетна комисия за изясняване на всички факти и обстоятелства около случая с източване на информация от електронната база данни на Националната Агенция за Приходите към 44-тото НС и предоставените останали документи по делото и въпреки взетите организационни мерки от НАП се е стигнало до конкретното изтичане на данни. „S. injectoin“ е идентифицирана като критична заплаха за сигурността минимум от 2007 година, когато излиза първата OWASP Top 10 Vulnerabilities L.. Големият риск от подобен тип атаки се дължи на лекотата, с която могат да бъдат засечени уязвимостите, както и лекотата, с която могат да бъдат експлоатирани тези уязвимости, за да компрометират сигурността на информацията.На база на изложеното и на база опита му в областта на информационната сигурност, ВЛ е категорично, че технически е било възможно предотвратяването на изтичане на данни към онзи момент.

От правна страна:

Искът е допустим-налице са положителните, съотв. липсват отрицателните условия, свързани със съществуването и упражняването правото на иск. Искът е предявен от процесуално правоспособна и дееспособна страна и срещу процесуално правоспособна страна /чл.205, ал.1 АП/, като не е налице и пречката по чл.39, ал.4 от специалния ЗЗЛД.

Разгледан по същество, искът е частично основателен, по следните съображения:

1. Съдебното производство е образувано е по искова молба /ИМ/ вх.№27810/16.09.19 г. по регистъра на АССГ, след разделяне на производството по адм.д.№10466/19 г. с определение от 20.09.19 г., в частта, с която от М. К. С., чрез пълномощника й-адв.С. Ю., е предявен иск, който съдът квалифицира, с правно основание чл.79, параграф 1 и чл.82, параграф 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на

физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), по реда на чл.203 и сл. АПК и чл.1 и сл. от ЗОДОВ, за осъждане на ответника Националната агенция по приходите да заплати на ищцата обезщетение в размер на 1000 лева за неимуществени вреди, настъпили от неправомерното бездействие на НАП да изпълни задължението си да защити по сигурен начин данните на ищцата като гражданин, станало причина да бъде допуснат пробив в информационната система на НАП, довело до публичното разкриване на личните данни на ищцата.

2. Фактическият състав, при осъществяването на който възниква правото на обезщетение за вреди, произтичащо пряко от член 82, параграф 1 от Общия регламент, включва претърпени материални или нематериални вреди настъпили в причинна връзка /в резултат на/ нарушение на задължения на ответника, които произтичат от чл. 24 и чл. 32 от Регламента за защита на данни, обуславят правна квалификация на иска по чл. 82, §1 вр. § 2 от от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

3. Релевантните факти по предявения иска са:

а/ Бездействие на ответника да изпълни задълженията си по произтичат от чл. 24 и чл. 32 от Регламента, при спазване на принципите за законосъобразност и добросъвестност, залегнали в чл. 5 § 1 б. "а", както и по б. "е" от същия, а именно: личните данни трябва да бъдат 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")

б/ настъпването на заявените от ищцата неимуществени вреди;

в/ пряка причинно-следствена връзка между заявеното фактическо основание на предявения иск-а/ и неимуществените вреди-б/.

Проекто-докладът по делото, включващ и разпределението на доказателствената тежест при точно изпълнение указанията на ВАС, е приет без възражения от страните.

В случая ответникът не се справи с носената от него доказателствена тежест да докаже че „не е отговорен за събитието, причинило вредата, тоест, че липсва нарушение, в причинна връзка, с което са претърпени вредите.“ По делото се установи точно обратното.

Разпоредбата на чл. 24 „Отговорност на администратора“ от с.р. предвижда, че като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствия с регламента. В допълнение, в чл. 32 са предвидени конкретните мерки които следва да се предприемат, а именно: "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: а) псевдонимизация и криптиране на личните данни; б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване; *в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент; г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.*

Администраторът на лични данни по см. на чл. 4 § 7 от ОРЗД и при обработване на личните данни, следва да спазва принципите за законосъобразност и добросъвестност, залегнали в чл. 5 § 1 б. "а", както и по б. "е", а именно*: личните данни трябва да бъдат 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*").

По делото се установи категорично от приетото и неоспорено от страните заключение на вещото лице, че източването на целия обем от 10.7 Gb данни не е осъществено еднократно, *а най- вероятно се е случвало в продължителен период от време*, каквато е честата практика на хакерите, с цел да не натоварват излишно засегнатите системи, при което могат да бъдат евентуално открити. Използвана е атака от тип „S. injectoin“ срещу едно от програмните приложения на сайта на НАП - “VAT refund“, като чрез този тип атака, *атакуващият се възползва от уязвимост в изходния код на конкретното уеб приложение и получава директен достъп до базата данни, което приложението използва, като предоставя административните данни за достъп до базата данни*. В конкретния случай чрез атака от тип „S. injectoin“срещу едно от програмните приложения на сайта на НАП - “VAT refund“ е получен нерегламентиран достъп до данните на 6 074 140 физически лица, с активна регистрация - 4 104 786 души, от които 24 507 чужденци и 4 057 328 души с активна регистрация и валидно ЕГН. Системите, от които е извършено източване на данни, са сървъри с операционна система W. server 2008R2 и база данни O. 11.2.02. O. неоторизиран достъп е засегнал всички бази данни на O. сървъра, към който има връзка уеб приложението “VAT refund“. За извършване на нерегламентирания достъп се използват публично достъпните функции на приложение или страница, като чрез него се подава специална команда, връщаща административните данни за достъп до базата данни. След получаването на тези данни, атакуващият се свързва директно към съответната База Данни и получава достъп до наличната информация в нея. В конкретния случай действията се дължат изцяло на външна намеса. Всяка организация е необходимо да изгради собствена С., включваща политики, правила и конкретни инструкции за осигуряване на

Информационната сигурност, базирано на Оценка на риска, направена на базата на конкретните процеси и информационни активи. *Една такава С. следва да бъде непрекъснато обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност.* Към момента на теча, НАП е бил разработила, внедрила и използвала С., изградена на основни правила, базирани на стандарта за информационна сигурност БДС 180/1ЕС 27001/2006 и в последствие актуализирана към по- новата версия БДС 180/1ЕС 27001/2014.

На база на тази С. са били определени и изпълнени преценените към онзи момент необходими и достатъчни технически и организационни мерки за защита на информацията, *но явно е пропуснато да бъде тествано конкретното приложение за атаки от типа* на „S. injectoin“ *при въвеждането му в експлоатация, както и не е бил извършван последващ контрол на сигурността на засегнатото W. приложение.*

Тези фактически установявания субсумират бездействие по смисъла на разпоредбата на чл. 24 „Отговорност на администратора“, като не са взети предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, изразяващо с в невъвеждането от администратора на *подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с регламента*. В допълнение, не са предприети предвидените в чл. 32, *в)* от Общия регламент конкретни мерки, а именно не са взети предвид достиженията на техническия прогрес, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица и не са приложени подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно:*процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.* В случая въведената С. не е била обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност. *„S. injectoin“ е била идентифицирана като критична заплаха за сигурността минимум от 2007 година, когато излиза първата* OWASP Top 10 Vulnerabilities L.. *Големият риск от подобен тип атаки се дължи на лекотата, с която могат да бъдат засечени уязвимостите, както и лекотата, с която могат да бъдат експлоатирани тези уязвимости, за да компрометират сигурността на информацията.При редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки, е било технически възможно предотвратяването на изтичане на данни към 2019 година.* Администраторът на лични данни по см. на чл. 4 § 7 от ОРЗД и при обработване на личните данни, не е спазил принципите за законосъобразност и добросъвестност, залегнали в чл. 5 § 1 б. "а", както и по б. "е" от Общия регламент, *а именно не е гарантирал подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване* и срещу случайна загуба, унищожаване или повреждане, *като не е приложил подходящи техническите и*

организационни мерки /“цялостност и поверителност“/.
Във връзка с доказване на твърдените вреди от ищцата са ангажирани, съотв. при първоначалното разглеждане на делото са събрани гласни доказателства, които запазват силата си, без да е необходимо повторното им събиране при новото разглеждане на делото.
Във връзка със заявените вреди, настоящият състав споделя разбирането, че в съответствие със съображения 1-во и 4-то за приемането на Общия регламент за защита на данните, защитата на физическите лица във връзка с обработването на лични данни е основно право. Член 8, параграф 1 от Хартата на основните права на Европейския съюз /„Хартата"/ и член 16, параграф 1 от Договора за функционирането на Европейския съюз /ДФЕС/ предвиждат, че всеки има право на защита на личните му данни. Обработването на лични данни следва да е предназначено да служи на човечеството.
След като е накърнено основно право на ищцата, като физическо лице при обработването на личните й данни от ответника като администратор-неприложени от администратора на лични данни подходящи технически и организационни мерки за осигуряване ниво на сигурност, съобразено с риска, 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, което е направило възможно пробива в информационните масиви на НАП, нормално е да се приеме, че ищцата изпитва неудобство, чувства се притеснено и несигурно. Накърнени са легитимните й очаквания спрямо държавата за сигурност в личната и имуществената й сфера, предвид общодостъпната информация за възможни злоупотреби с личните й данни оттук нататък.
По тези съображения, при установяване на този вид обичайни неимуществени вреди не бива да се изхожда само от формалните, външни доказателства. Да се приеме обратното и да се изисква формално пълно доказване на причинените неимуществени вреди, изразяващи се притеснението от всевъзможни бъдещи евентуални злоупотреби с личните данни на ищцата, означава да се отрече необходимостта от защитата на обществените отношения, свързани с обработването на лични данни, дадена с Общия регламент и ЗЗЛД. В случая в подкрепа на тези обичайни вреди са събраните по делото гласни доказателства чрез разпит на един свидетел, които съдът кредитира.
Съдът в няастоящия съдебен състав при излагане на изводите си възприема за приложима по аналогия практиката по чл.2 ЗОДОВ /Решение №63/18.03.16 г. на ВКС, ГК, III о. и решения към които то препраща-№ 480 от 23.04.2013 г. по гр. д. № 85/2012 г. на IV Г.О. на ВКС и № 165 от 16.06.2015 г. по гр.д. № 288/2015 г. на Трето ГО на ВКС./ Възприетото в т. II от ППВС № 4 от 23.12.1968 г. разрешение по въпроса за определянето на неимуществените вреди по справедливост не може да означава преценка по усмотрение на съда, която почива само на абстрактните представи на решаващия орган, тъй като тогава мотивите не биха могли да бъдат контролирани от

по-горестоящата инстанция. Затова съдът трябва да посочи конкретни факти, които според него са установени по делото и обосновават размера на неимуществените вреди. Това не означава, че при спецификата на непозволеното увреждане по чл.1 от ЗОДОВ е необходимо ищецът да докаже всички факти и обстоятелства, отразяващи се на неимуществените вреди. Когато се твърди причиняване на болки и страдания над обичайните за такъв случай, то тогава тези болки и страдания трябва изрично да бъдат посочени в исковата молба и да бъдат доказани.

В случая, с ненадлежното изпълнение, представляващо бездействие да се изпълнят точно задълженията за защита на личните данни, довело „нарушение на сигурността на лични данни"-нарушение на сигурността, което води до „неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин“, неизменно се причиняват вреди, които се изразяват в емоционални и психически терзания на личността.

Течът на лични данни неизменно е създал риск от злоупотреби с тези данни. Обективното наличие на риск не произтича от медийното му отразяване-не то създава риска. Рискът сам по себе си е вреда, ако този риск в евентуален бъдещ момент се реализира, просто вредата ще бъде по-голяма.

Да се отрича наличието на вреда, означава да се отрече необходимостта от защита на личните данни и същите да се признаят за общодостъпни. Колко и кои точно лични данни на ищцата са изтекли, което не се доказа по делото, също не сочи на липса на вреда, след като безспорно лични данни на ищцата са изтекли в публичното пространство.

Въпросът дали това неразрешено разкриване е станало възможно от успешно проведената хакерска атака и дали тя осъществява състав на престъпление е ирелевантен по делото-съдът не приравнява априори настъпилия противоправен резултат на противоправно бездействие на ответника, а съобразява процесуалните последици от проведеното по делото доказване. Не е налице основанието по чл.82, § 2 –ищецът не доказа, че по никакъв начин не е отговорен за събитието, причинило вредата. За да се освободи от отговорност, ответникът следваше да докаже, а той не успя, че е гарантирал подходящо ниво на сигурност на личните данни, включително срещу неразрешено или незаконосъобразно обработване, каквото представлява хакерската атака, чрез подходящи технически или организационни мерки. Установи се по делото, че такива са били предприети едва след осъществения пробив, довел до теча на лични данни на 6 074 140 физически лица, с активна регистрация - 4 104 786 души, от които 24 507 чужденци и 4 057 328 души с активна регистрация и валидно ЕГН, сред които и ищцата.

С оглед на изложеното, съдът приема, че ищцата може да претендира обезщетение за обичайните неимуществени вреди от бездействието на ответника да изпълни задължението си да защити по сигурен начин данните й като физическо лице, без да са нужни формални, външни доказателства за пълното установяване на тези обичайни вреди, тъй като те настъпват винаги в резултат от нарушаването сигурността на данните, което обективно създава риск за злоупотреба с тях и е нормално

лицето с нарушени права на защита да изпитва неудобство, несигурност и притеснение от този факт. В този случай размерът на обезщетението следва да се определи според стандарта на живот, за да не се превърне в източник на неоснователно обогатяване за пострадалия. Когато ищецът претендира вреди над обичайните, които са обусловени от конкретни, специфични обстоятелства, следва да ги посочи в исковата молба и безспорно да ги докаже. В случая ищцата не доказа вреди над обичайните, включително и с показанията на посочения от нея свидетел.

При съобразяване с естеството на увреждането и стандарта на живот / вкл.минимално установената работна заплата за страната за 2019 г.-560 лева/, съдът намира, че справедливото обезщетение за причинените обичайни вреди, които е търпяла в продължение на около 3 месеца, е в размер на 600 лева /чл.52 ЗЗД/ и уважава иска до този размер. В останалата му част- до пълния му предявен размер от 1000 лева-искът се отхвърля.

По отношение на искането за присъждането на законна лихва, съдът излага следното:

Законната лихва върху дължимото обезщетение има обезщетителен характер, но тя не е обезщетение за вредите от деликта, а обезщетение за забавено изпълнение на парично задължение /Решение №153 от 2.06.2015 г. по гр.д. №6735/14 г., IV г.о.

Деликвентът дължи обезщетение на пострадалото лице в размер на доказаните имуществени и неимуществени вреди, както и законна лихва от датата на увреждането/ чл. 84, ал. 3 ЗЗД/. Лихвите се дължат върху размера на обезщетението, защото съгласно цитираната разпоредба, деликвентът се счита в забава без покана, т.е. от датата на увреждането. В този случай присъждането на законната лихва е последица от уважаването на главния иск - за обезщетението и тъй като не се предявява като самостоятелен иск не се дължи държавна такса. Силата на присъдено нещо се разпростира върху главния иск, но не и върху размера на законната лихва. Размерът на законната лихва ще подлежи на установяване в изпълнителното производство. Не съществува пречка ищецът да предяви като самостоятелен иск обезщетение в размер на законната лихва по чл. 86 ЗЗД. В този случай ще се дължи заплащането на държавна такса на основание чл. 72, ал. 1 ГПК - съдът ще бъде сезиран с два обективно съединени иска и ще дължи произнасяне по всеки един от тях с решението, като силата на присъдено нещо ще се разпростира и върху притезанието по двата иска. / Определение 406/15.07.2009 г. на ВКС, Първо ТО по ч. т. д. 300/2009 г./

В случая, ищцата е избрала да не предяви самостоятелен иск за обезщетение за забава в размер на законната лихва от датата на увреждането до датата на подаване на исковата молба и предявеният иск е само един.В съответствие с приетото за установено от фактическа страна, съдът присъжда законната лихва върху уважената част от исковата претенция-600 лева от 15.07.2019 г.

При този изход на спора и на основание чл.10, ал.3 ЗОДОВ, вр.чл.226, ал.3 АПК съдът присъжда на ищцата разноски в размер общо на 45 лева-заплатени държавни такси. На процесуалния представител на ищцата-С. Ц. С.-Ю., осъществила процесуалното представителство на основание чл.38, ал.1, т.3 ЗА, ответникът следва на основание чл.38, ал.2 ЗА да заплати

възнаграждение за всички съдебни инстанции дотук /чл.226, ал.3 АПК/, което съдът определя в размер общо на 600 лева-чл.8, ал.1, т.1 от Наредба №1от 9.07.2004 г. за минималните размери на адвокатските възнаграждения.
Правото на разноски е възникнало и за ответника, съразмерно на отхвърлената част от иска, за защитата му осъществена от юрисконсулт пред всички съдебни инстанции дотук. Предвид обема и качеството на осъществената реално защита и броя на проведените заседания, съдът определя разноски в размер на 300 лева общо за всички съдебни инстанции дотук- чл.226, ал.3 АПК и чл. 37, ал.1 от Закона за правната помощ, във връзка с чл.25, ал.1 от Наредбата за заплащането на правната помощ, като съразмерно на уважената част от иска-чл.10, ал.4 ЗОДОВ, присъжда 120 лева.
Мотивиран така, Административен съд София-град-Второ отделение, 23-ти състав

Р Е Ш И:

ОСЪЖДА, по иска с правно основание по чл.79, параграф 1 и чл.82, параграф 1 от Регламент /ЕС/ 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО /Общ регламент относно защитата на данните/, Националната агенция по приходите да заплати на М. К. С. с [ЕГН], сумата в размер на 600 /шестстотин/ лева, представляваща обезщетение за неимуществени вреди, настъпили от неправомерното бездействие на ответника да изпълни задължението си да защити по сигурен начин данните на ищцата като физическо лице, позволило неоторизиран достъп и разкриване на лични данни на ищцата, оповестено публично на 15.07.2019 г., заедно със законната лихва върху тази сума, считано от датата на увреждането-15.07.2019 г. до окончателното изплащане на дължимото.
ОТХВЪРЛЯ иска до пълния му предявен размер за разликата до 1000 лева, като неоснователен.
ОСЪЖДА, на основание чл.10, ал.3 ЗОДОВ, вр.чл.226, ал.3 АПК, Националната агенция по приходите да заплати на М. К. С. с [ЕГН] сумата в размер на 45 /четиридесет и пет/ лева, заплатени държавни такси.
ОСЪЖДА, на основание чл.38, ал.2, вр.ал.1 т.3 ЗА, вр.чл.226, ал.3 АПК, Националната агенция по приходите да заплати на адвокат С. Ц. С.-Ю. –САК сумата в размер на 600 /шестстотин/ лева възнаграждение за осъщественото от нея безплатно процесуално представителство на ищцата
ОСЪЖДА, на основание чл.10, ал.4 ЗОДОВ, вр.чл.226, ал.3 АПК М. К. С. с [ЕГН] да заплати на Националната агенция по приходите сумата в размер на 120 /сто и двадесет/ лева, юрисконсултско възнаграждение за всички съдебни инстанции дотук, съразмерно на отхвърлената част от иска.

Решението може да се обжалва с касационна жалба пред Върховния административен съд в 14–дневен срок от съобщаването му на страните.
Решението да се съобщи на страните и СГП чрез изпращане на преписи

от него.

СЪДИЯ: