Р Е Ш Е Н И Е
№ 4979

гр. София, 25.09.2020 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 23 състав,** в публично заседание на 31.08.2020 г. в следния състав:

СЪДИЯ: Антоанета Аргирова

при участието на секретаря Емилия Митова и при участието на прокурора Десислава Кайнакчиева, като разгледа дело номер **11311** по описа за **2019** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е исково.

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. Й. И., [ЕГН], чрез пълномощника му-адв.С. Ю., е предявен иск 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 ищеца 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 ищеца като гражданин, станало причина да бъде допуснат пробив в информационната система на НАП, довело до публичното разкриване на личните данни на ищеца.

С ИМ ищецът твърди, че личните му данни се съхраняват и обработват от НАП, която е администратор на лични данни по смисъла на чл.4, т.7 от Общия регламент за защита на личните данни. Твърди още, че НАП е нарушила задълженията си по чл.59, ал.1, чл.45, ал.1, т.6, чл.64, чл.66, ал.1 и ал.2, чл.67, чл.68 ЗЗЛД, чл.24 и чл.32 от Общия регламент. На 15.07.2019 г. от медиите му станало известно, че при т.нар.

“хакерска атака“ от електронните масиви на НАП неправомерно е изтекла информация с голям обем, съдържащи лични данни на множество българи, в това число и неговите. НАП като държавен орган, отговарящ за приходите на държавата, без които държавата не би могла да функционира, следвало да е осигурила по безупречен начин своята сигурност, респ. в най-голяма степен да гарантира личните данни на гражданите на РБ.

С уточняваща молба от 22.10.2019 г. се конкретизира, че заявеното с ИМ искане за присъждане на законната лихва върху търсеното обезщетение от 1000 лева е от момента на подаване на ИМ-16.09.2019 г., в случая.

С уточняващата молба от 15.11.2019 г. се конкретизира, че се оспорва „бездействието на НАП да защити личните данни на ищеца и едновременно с това се предявява иск за обезщетение на причинените от това бездействие и предизвикано от него разпространение на личните му данни неимуществени вреди.“ Изрично се уточнява, че ответникът НАП макар и да е администратор на лични данни, е бездействал в качеството си на административен орган и носи отговорност по чл.1, ал.1 ЗОДОВ. Конкретното бездействие и нарушение на правни норми се изразявало в това, че НАП по силата на изрична законова разпоредба била длъжна да осъществи поведение /съвкупност от действия/, да предприеме такива мерки, че да гарантира и защити личните данни на ищеца. Съгласно чл.59, ал.1 ЗЗЛД, НАП като администратор на лични данни била длъжна, като отчита естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, да прилага подходящи технически и организационни мерки, за да гарантира, че обработването се извършва в съответствие с този закон. Същото задължение се съдържало и в чл.24 от Общия регламент, а в чл.32 от него се предвиждали конкретни мерки, които следвало да бъдат взети при администрирането и обработването на лични данни. Тези задължения били въведени, за да гарантират един от основните принципи на обработване на лични данни, прогласен в чл.5, § 1, б.“е“ от Общия регламент.

В случая ответникът не положил достатъчно грижа и не приложил ефективни мерки за защита на сигурността на данните, с което не изпълнил задълженията си по чл.24 и чл.32 от Общия регламент и чл.59, ал.1 ЗЗЛД. Ответникът нарушил и разпоредбите на чл.45, ал.1, т.6 ЗЗЛД, които го задължават личните данни да се обработват по начин, който гарантира подходящо ниво на сигурност, като се прилагат подходящи технологии и организационни мерки; чл.64 ЗЗЛД, който го задължава да извършва оценка на въздействието на предвидените операции по обработването на лични данни върху тяхната защита; чл.66, ал.1 и ал.2 ЗЗЛД, който го задължава отчитайки достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, да прилага подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност; чл.67 ЗЗЛД-в случаите на нарушение на сигурността на личните данни, което има вероятност да доведе до риск за правата и свободите на субектите на данни, администраторът без излишно забавяне, но не по-късно от 72 часа след като е разбрал за нарушението, уведомява комисията за него; чл.68 ЗЗЛД-когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на субектите на данни, да уведоми субекта на данните за нарушението не по-късно от 7 дни от установяването му.

Твърди се, че така изброените нарушения са довели до регламентираното в § 1, т.10 от ДР на ЗЗЛД, вр.чл.4, т.12 от Общия регламент понятие: "Нарушение на сигурността на лични данни", което означавало нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.
Неправомерно разкритите данни били имена, ЕГН, адрес, номер на документа за самоличност, данни за доходите. В резултат на това били причинени неимуществени вреди, изразяващи в чувството на застрашеност, притеснение, което продължавало, опасение, че с личните му данни ще бъде злоупотребено, като евентуалните възможности за това са много-да не бъде отчуждено имуществото му, злоупотребено с банковите му сметки или изтеглени кредити от негово име, да не бъде променено гражданското му състояние, да бъде откраднатa самоличността му и използвана по всевъзможни начини, които биха навредили на ищеца. До настоящия момент ищецът срещнал в медиите множество плашещи материали за това как биха могли да бъдат използвани личните му данни, като специалисти определяли този случай за дори по-лош от Ч., тъй като не се знаело кога във времето и по какъв начин ще бъде злоупотребено с личните данни. Всичко това натоварвало психически ищеца изключително много. Чувствал се незащитен от държавата. Страхувал се да не бъде изнудван, заплашван, нападнат физически или отвлечен, с оглед изтеклите данни за неговите доходи и адреса му. Тези притеснения повлияли в негативен аспект на нормалния ритъм на живот на ищеца, като той перманентно е напрегнат, стресиран и уплашен.
С писмения отговор на исковата молба ответникът оспорва допустимостта и основателността на иска.
В о.с.з. пред АССГ ищецът се представлява от адвокати Ю. и Ю., който пледират за уважаването на иска и за присъждането на разноските за съдебното производство.
Ответникът, чрез процесуалния си представител-юрк.Т., моли за отхвърлянето на иска като недоказан. Твърди, че събраните по делото доказателства установявали, че НАП е предприела всички необходими и организационни мерки за защита при обработването на личните данни.
Участващият по делото прокурор от Софийска градска прокуратура дава заключение за неоснователност на предявения иск., Счита, че не са налице кумулативните предпоставки на чл. 1 от ЗОДОВ. Не било установено по несъмнен начин твърдяното неправомерно бездействие от страна на НАП да защити по сигурен начин данните на гражданите. В конкретния случай били представени редица доказателства за редица действия предприети от ответника. В този смисъл твърдяното в исковата молба бездействие не било налице. Не била доказана причинно-следствена връзка между изтичането на лични данни и твърдените вреди. В случая лицата още в исковата молба твърдели, че са узнали от медийни публикации, не била налице пряка причинно-следствена връзка, а косвена, за която ответникът не отговарял. Алтернативно заема позиция, че размерът на исковата претенция е завишен и не съответства на чл.52 ЗЗД.
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.

По делото се представи извадка от получен SMS от дата 09.08.2019 г., със следното съдържание: „НАП: По заявка номер 6877 ИМА неправомерно разкрити лични данни“. Не е посочен телефонния номер, на който е получен посоченият SMS.

От справка на НАП от 02.07.2020 г. е видно, че за идентификатор [ЕГН] /ЕГН на ищеца /М. Й. И./ са разкрити лични данни, които включват ЕГН и имена и данни за изплатени доходи на физически лица за 2007 г. и за 2008 г.

По делото са приети писмени доказателства, от които се установява, че след изтичането на лични данни от информационните масиви на НАП, последната е информирала за това Софийската градска прокуратура и Комисията за защита на личните данни.

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 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 СУСИ по стандарт БДС ISO/IEC 27001:2006 в НАП. В НАП е изработена Методика за оценка на риска, версия 1, към м. декември 2013 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 ЗНАП“, „Указания за обозначаване и работа с информация“, „Указания за попълване на образци на процедура“, „Указания за попълване на образеца на инструкция“ и др.

Видно от предоставена от Комисията за защита на личните данни / КЗЛД/ с нейно писмо изх.№ППН-01-1744/2019 г.#1 от 14.11.2019 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 ищеца. Видно е още и това, че в хода на извършена от страна на КЗЛД проверка за изтеклата информация от информационните масиви на НАП, е установено, че при осъществяване на дейността си, НАП в качеството си на администратор на лични данни, не е приложила подходящи технически и организационни мерси, в резултат на което е осъществен неоторизиран достъп, неразрешено разкриване и разпространение

на лични данни на физически лица, в различен обем. За така установеното, председателят на КЗЛД е издал НП против НАП за нарушение на чл. 32, § 1, б. „б“ от Общия регламент относно защитата на личните данни. НП не е влязло в сила, предвид оспорването му пред СРС. Отделно от това, предвид констатирани нарушения, с Решение № ППН-02-399/22.08.2019 г. по описа на КЗЛД, на НАП е издадено и разпореждане за предприемане на подходящи технически и организационни мерки. Решението е оспорено пред АССГ, като е образувано адм. дело №10477/2019 г., което е висящо и не е приключило с окончателен съдебен акт

С молба от 06.07.2020 г. ответникът чрез процесуалния си представител изрично отказа да формулира задачи към вещо лице. При това положение, след като с протоколно определение от 22.06.2020 г. е разпределил доказателствената тежест между страните, допуснал е служебно СТЕ и изрично е указал последиците при неформулиране на задачи за ВЛ, съдът с определение от з.з. на 09.07.2020 г. отмени определението си за допускане извършването на СТЕ от вещо лице със специалност „киберсигурност“. Последиците от отказа на ответника за СТЕ, съдът ще изложи и аргументира по-долу в правните си изводи по спора.

По делото са събрани гласни доказателства, чрез разпит на свидетеля Д. А. А.. От показанията му е видно, че ищецът е изпитвал притеснения за изтеклите му лични данни. Впечатленията на свидетеля са преки и непосредствени и произтичат от комуникацията му са с ищеца, с когото са псалтикийни певци-свидетелят пее в хора на църквата „Св.А.“, а ищецът в църквата „Св.П.“

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:

Дадената от съда в доклада по делото правна квалификация на предявения иск по чл.79, параграф 1 и чл.82, параграф 1 от Регламент /ЕС/ 2016/679 /Общ регламент относно защитата на данните/, по реда на чл.203 и сл. АПК и чл.1 и сл. от ЗОДОВ е в съответствие с Определение №4991/28.04.2020 г. по дело №3504/20 г. на ВАС, V о., Определение № 5000/28.04.2020 г. по дело №3502/20 г. на ВАС, V о., Определение № 5277/04.05.2020 г. по дело №3498/20 г. на ВАС, V о., Определение № 5210/30.04.2020 г. по дело №3499/20 г. на ВАС, V о., Определение №5898/21.05-2020 г. по дело №3497/20 г. на ВАС, V о., Определение №5165/29.04.2020 г. по дело №3496/20 г. на ВАС, V о., Определение № 2732/20.02.20 г. по дело №1007/20 г. на ВАС, V о., Определение №3332/04.03.2020 г. по дело №1132/2020 г. на ВАС, V о. и др.

Във фактическия състав на предявения иск се включват следните елементи:

- бездействие на орган или длъжностно лице на НАП да защити по сигурен начин данните на ищеца, изразяващи се в неизпълнение на задълженията му по чл.59, ал.1, чл.45, ал.1, т.6, чл.64, чл.66, ал.1 и ал.2, чл.67, чл.68 ЗЗЛД, чл.24 и чл.32 от Общия регламент;
- неимуществени вреди, заявени с исковата молба
- пряка причинно-следствена връзка между бездействието за изпълнение на законовите задължения и настъпването на вредата за ищеца.

Разпоредбите, с които ищецът обосновава бездействие за изпълнение на законови задължения на ответника, са със следното съдържание:
ЗЗЛД:
Чл. 59. (Нов – ДВ, бр. 17 от 2019 г.) (1) Администраторът на лични данни, като отчита естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, прилага подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с този закон. При необходимост тези мерки се преразглеждат и актуализират.
Чл. 45. (Нов – ДВ, бр. 17 от 2019 г.) (1)При обработването на лични данни за целите по чл. 42, ал. 1 / Правилата на тази глава се прилагат при обработването на лични данни от компетентни органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване/ личните данни трябва да:
…
т.6 се обработват 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.
Чл.64(Нов – ДВ, бр. 17 от 2019 г.) (1) Когато има вероятност определен вид обработване, по-специално това при което се използват нови технологии и предвид естеството, обхвата, контекста и целите на обработването, да доведе до висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът на лични данни извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.
(2) Оценката по ал. 1 съдържа най-малко общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и за доказване на съответствие с правилата на тази глава, като се вземат предвид правата и законните интереси на субектите на данните и другите засегнати лица.
Чл. 66. (Нов – ДВ, бр. 17 от 2019 г.) (1) Администраторът и обработващият лични данни, като отчитат достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, по-специално по отношение на обработването на категориите лични данни по чл. 51, ал. 1 /Обработването на лични данни, разкриващо расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравословното състояние или сексуалния живот и сексуалната ориентация на лицето, е разрешено, когато това е абсолютно необходимо, съществуват подходящи гаранции за правата и свободите на субекта на

данни и е предвидено в правото на Европейския съюз или в законодателството на Република България/.
(2) По отношение на автоматизираното обработване администраторът или обработващият лични данни след оценка на рисковете прилага мерки, имащи за цел:
1. контрол върху достъпа до оборудване – да се откаже достъп на неоправомощени лица до оборудването, използвано за обработване на лични данни;
2. контрол върху носителите на данни – да се предотврати четенето, копирането, изменянето или отстраняването на носители на данни от неоправомощени лица;
3. контрол върху съхраняването – да се предотврати въвеждането на лични данни от неоправомощени лица, както и извършването на проверки, изменянето или изтриването на съхранявани лични данни от неоправомощени лица;
4. контрол върху потребителите – да се предотврати използването на автоматизирани системи за обработване от неоправомощени лица чрез използване на оборудване за предаване на данни;
5. контрол върху достъпа до данни – да се гарантира, че лицата, на които е разрешено да използват автоматизирана система за обработване, имат достъп само до личните данни, които са обхванати от тяхното разрешение за достъп;
6. контрол върху комуникацията – да се гарантира възможността за проверка и установяване на кои органи са били или могат да бъдат предадени лични данни, или кои органи имат достъп до лични данни чрез оборудване за предаване на данни;
7. контрол върху въвеждането на данни – да се гарантира възможността за последваща проверка и установяване на това какви лични данни са били въведени в автоматизираните системи за обработване, както и кога и от кого те са били въведени;
8. контрол върху пренасянето – да се предотврати четенето, копирането, изменянето или изтриването на лични данни от неоправоомощени лица при предаването на лични данни или при пренасянето на носители на данни;
9. възстановяване – да се гарантира възможността за възстановяване на инсталираните системи в случай на отказ на функциите на системите;
10. надеждност – да се гарантира изпълнението на функциите на системата и докладването за появили се във функциите дефекти;
11. цялостност – да се гарантира недопускане на увреждане на съхраняваните лични данни вследствие на неправилно функциониране на системата.
Чл. 67. (Нов – ДВ, бр. 17 от 2019 г.) (1) В случай на нарушение на сигурността на личните данни, което има вероятност да доведе до риск за правата и свободите на субектите на данни, администраторът без излишно забавяне, но не по-късно от 72 часа след като е разбрал за нарушението, уведомява комисията, съответно инспектората, за него. Когато уведомлението е подадено след срока по изречение първо, в него се посочват причините за забавянето.
(2) Обработващият лични данни уведомява администратора без излишно

забавяне, но не по-късно от 72 часа след като е установил нарушение на сигурността на лични данни.
(3) Уведомлението по ал. 1 съдържа най-малко:
1. описание на нарушението на сигурността на личните данни, включително когато е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;
2. името и координатите за връзка на длъжностното лице по защита на данните или на друго звено за контакт, от което може да се получи повече информация;
3. описание на евентуалните последици от нарушението на сигурността на личните данни;
4. описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.
(4) Когато не е възможно информацията да се подаде едновременно, тя може да се подаде поетапно без по-нататъшно ненужно забавяне.
(5) Администраторът документира всяко нарушение на сигурността на личните данни по ал. 1, като включва фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него.
(6) Когато нарушението на сигурността на личните данни засяга лични данни, които са изпратени от или на администратор от друга държава – членка на Европейския съюз, информацията по ал. 3 се съобщава на този администратор без излишно забавяне, но не по-късно от 7 дни от установяването на нарушението.
Чл. 68. (Нов – ДВ, бр. 17 от 2019 г.) (1) Когато има вероятност нарушението на сигурността на личните данни по чл. 67, ал. 1 да доведе до висок риск за правата и свободите на субектите на данни, администраторът на лични данни уведомява и субекта на данните за нарушението не по-късно от 7 дни от установяването му.
(2) В уведомлението по ал. 1 на ясен и разбираем език се посочва описание на нарушението и най-малко информацията и мерките по чл. 67, ал. 3, т. 2, 3 и 4.
(3) Субектът на данните не се уведомява за нарушение по ал. 1, ако е изпълнено някое от следните условия:
1. администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението, по-специално мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране;
2. администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни;
3. уведомяването би довело до непропорционални усилия; в този случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да са в еднаква степен ефективно информирани.

(4) Когато администраторът не е уведомил субекта на данните за нарушението на сигурността на личните данни по ал. 1, комисията, съответно инспекторатът, след като отчете каква е вероятността нарушението да породи висок риск, може да изиска от администратора да уведоми субекта на данните.
(5) В случаите по чл. 54, ал. 3 администраторът може да не уведоми субекта на данните за нарушението по ал. 1, да го уведоми след срока по ал. 1, както и да ограничи информацията по ал. 2.

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)

Член 4

Определения

12) „нарушение на сигурността на лични данни" означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

Член 24

Отговорност на администратора

1. 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 съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират.
2. Когато това е пропорционално на дейностите по обработване, посочените в параграф 1 мерки включват прилагане от страна на администратора на подходящи политики за защита на данните.
3. Придържането към одобрени кодекси за поведение, посочени в член 40 или одобрени механизми за сертифициране, посочени в член 42 може да се използва като елемент за доказване на спазването на задълженията на администратора.

Член 32

Сигурност на обработването

1. 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.
2. При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.
3. Придържането към одобрен кодекс за поведение, посочен в член 40 или одобрен механизъм за сертифициране, посочен в член 42 може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграф 1 от настоящия член.
4. Администраторът и обработващият лични данни предприемат стъпки всяко физическо лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до лични данни, да обработва тези данни само по указание на администратора, освен ако от въпросното лице не се изисква да прави това по силата на правото на Съюза или правото на държава членка.
Съгласно чл.154, ал.1 ГПК, вр. чл.204, ал.5 АПК, всяка страна е длъжна да установи фактите, на които основава своите искания или възражения.
По отношение на първия елемент от фактическия състав на предявения иск /бездействие на орган или длъжностно лице на НАП да защити по сигурен начин данните на ищеца, изразяващи се в неизпълнение на задълженията му по чл.59, ал.1, чл.45, ал.1, т.6, чл.64, чл.66, ал.1 и ал.2, чл.67, чл.68 ЗЗЛД, чл.24 и чл.32 от Общия регламент/, което ищецът оспорва преюдициално в исковото производство, той е в положението на ищец по отрицателен установителен иск. Ищецът следва да установи наличието на свое защитимо право, засегнато от правния спор, като докаже фактите, от които то произтича. Единствено ответникът ще е длъжен да доказва изпълнението на действията, дължими от ответника по силата на посочените от ищеца законови норми, обезпечаващи защитимото право на ищеца. Ищецът ще се задоволи само с възраженията си, че такова изпълнение не е осъществено /Тълкувателно решение № 8 от 27.11.2013 г. на ВКС по тълк. д. № 8/2012 г., ОСГТК/.
С оглед законово дължимото поведение от ответника, съдът разпредели доказателствената тежест между страните, като по отношение установяването на първия елемент от фактическия състав на предявения иск я възложи на ответника. Изрично му указа, предвид носената от него доказателствена тежест, че за установяване изпълнението на задълженията му са необходими специални знания от специалност „киберсигурност“, с които съдът не разполага, и му даде възможност да формулира задачи за вещото лице по допусната служебно СТЕ.
С оглед изричния отказ на ответника да го направи, вкл. демонстративния отказ за възприемане съдебния акт за разпределение на доказателствената тежест между страните по делото, съдът намира, че ответникът не се справи с носената от него доказателствена тежест и не установи, че извършените от него действия /за които ангажира само писмени доказателства/, са били подходящи технически за осигуряване на съобразено с риска ниво на

сигурност на личните данни на ищеца.
Последицата от процесуалното поведение на ответника е приемането за установен по делото на първия елемент от фактическия състав на предявения иск- бездействие за точно изпълнение на задължението по чл.59 ЗЗЛД и чл.32 от Общия регламент относно защита на данните, а именно приложени от администратора на лични данни подходящи технически мерки за осигуряване на 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.
По отношение на втория и третия елемент от фактическия състав на предявения иск-неимуществена вреда и пряка причинно-следствена връзка между бездействието и вредата, съдът излага следното:
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 ищеца при обработването на личните му данни от ответника като администратор-неприложени от администратора на лични данни подходящи технически мерки за осигуряване на 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 изглежда да е направило възможно пробива в информационните масиви на НАП, нормално е да се приеме, че ищецът изпитва неудобства, чувства се притеснено и несигурно. Накърнени са легитимните му очаквания спрямо държавата за сигурност в личната и имуществената му сфера, предвид общодостъпната информация за възможни злоупотреби с личните му 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 ищеца, 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 и събраните по делото свидетелски показания. Съдът в този 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.

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 непроведеното от него успешно пълно доказване на надлежно изпълнение на задължението му за сигурност на обработването.

Ако беше провел успешно доказване на надлежно изпълнение на задължението, ответникът би се освободил от отговорност по ЗОДОВ спрямо ищеца за настъпилия противоправен резултат. Пряката причинно-следствена връзка, обратно на заключението на прокурора, не се прекъсва от факта как е узнал ищеца за настъпилия „теч на лични данни“. Още повече, че уведомяването му е дължимо, и то от ответника.

В обобщение съдът приема, че ищецът може да претендира обезщетение за обичайните неимуществени вреди от бездействието на ответника да изпълни задължението си да защити по сигурен начин данните му като физическо лице, без да са нужни формални, външни доказателства за установяване на тези обичайни вреди, тъй като те настъпват винаги в резултат от нарушаването сигурността на данните. 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, той следва да ги посочи в исковата молба и безспорно да ги докаже. В случая ищецът не доказа вреди над обичайните.

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 претърпените обичайни вреди е в размер на 500 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.
При този изход на спора и на основание чл.10, ал.3 ЗОДОВ съдът присъжда разноски за първоинстаницонното съдебно производство в размер на 160 лева, както следва:на ищеца в размер на 10 лева-заплатена държавна такса и 150 лева, съразмерно на уважената част от иска, на адвокат С. Ц. С.-Ю. по чл.38, ал.1, т.3, вр.ал.2 от ЗА, в съотв. с приложения по делото договор за правна защита и съдействие.
Правото на разноски е възникнало и за ответника, съразмерно на отхвърлената част от иска, за защитата му осъществена от юрисокнуслт, но такива с решението не се възлагат върху ищеца /чл.172а, т.7 АПК/, поради липса на своевременно направено искане за това-чл.10, ал.4 ЗОДОВ и чл.81 ГПК, вр чл.144 АПК.
Мотивиран така, АССГ II о., 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. Й. И., [ЕГН] сумата в размер на 500 /петстотин/ лева, представляваща обезщетение за неимуществени вреди, настъпили от неправомерното бездействие на ответника да изпълни задължението си да защити по сигурен начин данните на ищеца като физическо лице, позволило неоторизиран достъп и разкриване на личните данни на ищеца, оповестено публично на 15.07.2019г., заедно със законната лихва върху тази сума, считано от датата на подаване на исковата молба-16.09.2019 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, Националната агенция по приходите да заплати на М. Й. И., [ЕГН] сумата в размер на 10 лева, заплатена държавна такса за предявения иск.
ОСЪЖДА, на основание чл.38, ал.1, т.3, вр.ал.2 от ЗА, вр.чл.10, ал.3 ЗОДОВ, Националната агенция по приходите да заплати на адвокат С. Ц. С.-Ю. с адрес на упражняване на дейността в [населено място], бел.“В.“ №1А, Търговски дом, ет.3, к.308, сумата в размер на 150 /сто и петдесет/ лева, съразмерно на уважената част от иска, адвокатско възнаграждение.

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: