

РЕШЕНИЕ

№ 9510

гр. София, 21.06.2024 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, Второ отделение 32 състав,
в открито заседание на 19.04.2024 г. в следния състав:

СЪДИЯ: Красимира Милачкова

при участието на секретаря Антонина Митева, като разгледа дело номер **710** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 203 - 207 от Административно процесуалния кодекс (АПК)

Образувано е по иск, предявен от Г. Д. Г. против Националната агенция за приходите /НАП/, за сумата 1000 лева, представляваща обезщетение на неимуществени вреди. Последните се сочат за произтекли от неизпълнение на задължения на администрацията относно защитата на личните данни. Предявеният иск е с правно основание чл. 82, § 1, вр. § 2 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 (ОРЗД). Ищцата твърди, че на 15.07.2019г. разбрала от медиите, че при т. н. „хакерска атака“ от електронните масиви на НАП неправомерно е била изтеглена информация с голям обем, съдържащ лични данни на множество български граждани и граждани на Европейския съюз. На 25.07.2019г. се уведомила от приложението на агенцията, че нейни лични данни са били неправомерно изтеглени и е станала обект на това посегателство. Ищцата претърпяла негативни изживявания и се опасява от бъдеща злоупотреба с лични данни, поради което моли да бъде обезщетена с горепосочената сума. Претендира и законна лихва, считано от 15.07.2019г. до окончателното изплащане на задължението.

Ответникът НАП оспорва иска като неоснователен. Твърди, че е изпълнил всички свои задължения, произтичащи от ОРЗД и националното законодателство, гарантиращи сигурна защита на администрираните от него лични данни. Навежда

доводи, че разкритите данни са в резултат на престъпление и не се дължат на негово неправомерно бездействие. Сочи, че всички технически средства и софтуер са съобразени със съвременните средства за защита и достиженията на техническия прогрес. Претендира юрисконсултско възнаграждение.

Съдът в настоящия състав, като обсъди доводите на страните и прецени събраните по делото доказателства, приема следното от фактическа и правна страна.

На 15.07.2019г. неизвестно лице е осъществило нерегламентиран достъп до информационната система на НАП, станал известен като „хакерска атака“, вследствие на което е разпространена информация, съдържаща личните данни на множество българи. По делото е представена извадка от официалната интернет страница на НАП (check.nra.bg/ker/), видно от която за подадения идентификатор [ЕГН] има разпространени данни. Последните включват ЕГН и имена; данни от справка за изплатени доходи на физически лица за 2015г.

Видно от представените от ответника писмени доказателства, последният е предприел организационни и технически мерки за защита на администрираните от агенцията данни. 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“. Със Заповед № ЗЦУ-586/30.04.2014 г. на изпълнителния директор на НАП е наредено да се внедри система за управление на сигурността на информацията (С.) по стандарт БДС ISO/IEC 27001:2006 в НАП. Утвърдена е Политика по информационна сигурност на НАП. Приета е Методика за анонимизиране на индивидуални данни, версия 1, към 01.2017 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.

По делото са представени и Заповед № ЗЦУ-733/17.06.2016 г. на изпълнителния директор на НАП, с която са утвърдени „Процедури с приложения към тях на отдел „Превенция на финансовата и информационна система“ в Инспекторат на НАП, „Вътрешни правила за мрежовата и информационна сигурност, а именно: Правила за ползване на електронна поща и Интернет в НАП, версия 3.0; Правила за ползване на мрежови файлови ресурси в НАП, версия 2.0; Правила за правата и задълженията на потребителите, ползващи информационни активи в НАП, версия 2.0; Правила за работа от разстояние в НАП, версия 2.0; Правила за работа с преносими информационни активи в НАП, версия 2.0; Правила за управление на достъпа до информационни активи и услуги в НАП, версия 2.0. Със същата заповед е утвърдена и „Политика по информационна сигурност на НАП“, версия 3.0. Представена е и Заповед № ЗЦУ-83 от 23.01.2013 г. на изпълнителния директор на НАП, с която са определени вида, съдържанието, реда за създаване, поддържане и достъп до регистъра на НАП и базите данни за задължените лица, формата и елементите на данъчно-осигурителната сметка и сроковете за съхранение на архивираната информация. Изготвен е списък на видовете операции по обработване на лични данни,

за които се изисква извършване на оценка на въздействието върху защитата на данните съгласно чл. 35, пар. 4 от Регламент (ЕС) 2016/679. По делото са представени и Вътрешни правила за оборот на електронни документи и документи на хартиен носител в НАП, утвърдени със Заповед № ЗЦУ-535/11.05.2016 г. на изпълнителния директор на НАП. С представената заповед № ЗЦУ-746/25.05.2019г. изпълнителният директор на НАП е утвърдил Политика по защита на личните данни, а с негова предходна заповед № ЗЦУ-1595/29.11.2017г. са дадени указания за обозначаване и работа с информацията. Представени са подробни процедури, съответно: ПФИС 3. Версия Г Извършване на действия при съмнения за инцидент, касаещ информационната сигурност; ПФИС 7, Версия В Оценка на риска за информационната сигурност; Процедура ПФИС 11, Версия В Извършване на коригиращи действия по С..

С определение от 27.03.2024г. е допуснато изслушване показанията на свидетел при довеждането му от ищцата, за претърпените от нея вреди. В следващо открито съдебно заседание свидетелят не е доведен и предвид липсата на други искания, определението за допускането му е отменено.

При така установените факти, съдът в настоящия състав приема, че искът е допустим като предявен от активно легитимирано лице срещу надлежен ответник съобразно чл.205, ал.1 АПК, тъй като съгласно чл.2, ал.2 от Закона за НАП (ЗНАП), агенцията е юридическо лице. Разгледан по същество, искът е неоснователен.

Искът е с правно основание чл.82 §1 вр. §2 от ОРЗД и следва да бъде разгледан по реда на чл. 203 и сл. от АПК. В споровете от този вид не намира приложение чл.1 от Закона за отговорността на държавата и общините за вреди – така, в решения № 7720/28.06.2021г. по адм. д. № 10801/2020г., № 6661/03.06.2021 г. по адм. д. № 11286/2020 г., № 6350/27.05.2021 г. по адм. д. № 8821/2020 г. на Върховния административен съд, Трето отделение. Посочва се в цитираните решения, че: „Съгласно чл. 39, ал. 1 ЗЗЛД, при нарушаване на правата му по Регламент (ЕС) 2016/679 и по закона субектът на данни може да обжалва действия и актове на администратора и на обработващия лични данни пред съда по реда на Административнопроцесуалния кодекс. В производството по ал. 1 субектът на данни може да иска обезщетение за претърпените от него вреди вследствие на неправомерно обработване на лични данни от страна на администратора или на обработващия лични данни - чл. 39, ал. 2 ЗЗЛД. В чл. 39, ал. 1 ЗЗЛД не се съдържа специална процесуална уредба относно реда за упражняване на правото на субекта да сезира съда за нарушените му права при обработване на личните му данни, а се препраща към общия административнопроцесуален закон за търсене на отговорност на всички администратори на лични данни, независимо от тяхната правосубектност и притежавани качества (публични органи или частноправни субекти), по аргумент от § 1, т. 1 АПК. Процесуалният ред, по който засегнатият субект може да търси обезщетение и отговорност за причинените вреди поради неправомерно обработване на личните му данни, е уреден в глава единадесета "Производство за обезщетения" на Административнопроцесуалния кодекс“.

Правото на ефективна съдебна защита срещу администратор или обработващ лични данни е уредено в чл. 79 §1 ОРЗД, според който без да се засягат които и да било налични административни или несъдебни средства за защита, включително правото на подаване на жалба до надзорен орган съгласно член 77, всеки субект на данни има право на ефективна съдебна защита, когато счита, че правата му по настоящия

регламент са били нарушени в резултат на обработване на личните му данни, което не е в съответствие с настоящия регламент. По силата на чл. 82 § 1 ОРЗД всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди.

Съгласно чл. 203, ал. 1 от Глава XI на АПК, исковите за обезщетения за вреди, причинени на граждани или юридически лица от незаконосъобразни актове, действия или бездействия на административни органи и длъжностни лица се разглеждат по реда на тази глава. Съгласно чл. 203, ал. 3 от АПК, по реда на тази глава се разглеждат и исковите за обезщетения за вреди, причинени от достатъчно съществено нарушение на правото на Европейския съюз. Материалноправните предпоставки за отговорността на държавата за вреди, причинени от нарушение на правото на ЕС, произтичат директно от наднационалния правен ред.

Основателността на исковата претенция, предполага установяването на кумулативното наличие на следните предпоставки: 1) незаконосъобразно бездействие на ответника в нарушение на ОРЗД 2) претърпяна вреда – в случая, неимуществена; 3) причинна връзка - пряка и непосредствена такава между незаконосъобразното бездействие и вредоносния резултат.

Първата предпоставка за ангажиране отговорността на ответника е наличие на бездействие и това бездействие да е в нарушение на изискванията на ОРЗД. В случая, релевантна за спора е информацията, станала достъпна на 15.07.2019 г. вследствие нерегламентиран достъп до електронните масиви на НАП, съдържаща лични данни на ищцата. В резултат на това се твърдят възникнали притеснения и опасения у ищцата да не бъде злоупотребено с тези данни. „Лични данни“, към времето на обработването им – м. юли 2019г., съгласно чл.4, §1 от ОРЗД, са: всяка информация свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице. Обработване на лични данни по смисъла на Регламента (чл.4, §2) означава 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. В релевантния период условията за допустимост при обработване на личните данни са изрично регламентирани в чл.6 от Регламент (ЕС) 2016/679. Съгласно тази разпоредба обработването е законосъобразно, само ако и доколкото е приложимо поне едно от условията, изрично и изчерпателно посочени в б. „а“ – „е“: а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели; б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор; в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора; г)

обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице; д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора; е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете. Според чл.24 от ОРЗД, 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 със същия регламент. Тези мерки се преразглеждат и при необходимост се актуализират, а в чл. 32 са предвидени конкретните мерки които следва да се предприемат. Задължението да докаже, че обработването на личните данни се извършва в съответствие с изискванията на Регламента е на администратора. Обстоятелството, че е изтекла информация от сървърите на НАП вследствие неоторизиран достъп е факт, безспорен по делото. Той обаче сам по себе си не обуславя извод, че е налице неизпълнение на задължения на администратора, произтичащи от посочените разпоредби, да осигури достатъчна надеждност и сигурност на информационната си система, да защити физическите лица във връзка с обработването на личните им данни по смисъла на ОРЗД, в т. ч. правото на защита на личните им данни.

В решение от 14.12.2023 г. по дело С-340/21 Съдът на Европейския съюз посочва, че членове 24 и 32 от ОРЗД трябва да се тълкуват в смисъл, че неразрешено разкриване на лични данни или неразрешен достъп до такива данни от „трета страна“ по смисъла на член 4, точка 10 от този регламент сами по себе си не са достатъчни, за да се приеме, че приложените от съответния администратор технически и организационни мерки не са „подходящи“ по смисъла на тези членове 24 и 32. Последният трябва да се тълкува в смисъл, че преценката дали приложените от администратора технически и организационни мерки по този член са подходящи трябва да бъде направена от националните юрисдикции конкретно, като се вземат предвид рисковете, свързани със съответното обработване, и като се прецени дали естеството, обхватът и прилагането на тези мерки са съобразени с тези рискове. Принципът на отчетност на администратора, закрепен в член 5, параграф 2 и конкретизиран в член 24 от ОРЗД, трябва да се тълкува в смисъл, че в исково производство за обезщетение по член 82 от този регламент разглежданият администратор носи тежестта за доказване на обстоятелството, че приложените от него мерки за сигурност по член 32 от посочения регламент са подходящи. Член 32 от ОРЗД и принципът на ефективност на правото на Съюза трябва да се тълкуват в смисъл, че за да се прецени дали са подходящи мерките за сигурност, приложени от администратора на основание на този член, назначаването на съдебна експертиза не може да представлява доказателствено средство, което системно е необходимо и достатъчно. Член 82, параграф 3 от ОРЗД трябва да се тълкува в смисъл, че администраторът не се освобождава от задължението си по член 82, параграфи 1 и 2 от този регламент за обезщетяване на претърпените от дадено лице вреди само поради факта, че тези вреди произтичат от неразрешено разкриване на лични данни или неразрешен достъп до такива данни от „трета страна“ по смисъла

на член 4, точка 10 от посочения регламент, като посоченият администратор трябва тогава да докаже, че причинилият съответните вреди факт не може по никакъв начин да му бъде вменен. Член 82, параграф 1 от същия Регламент трябва да се тълкува в смисъл, че опасенията, които субект на данни изпитва, вследствие на нарушение на този регламент, от потенциална злоупотреба с неговите лични данни от трети лица, могат сами по себе си да представляват „нематериална вреда“ по смисъла на тази разпоредба.

Като извърши преценка в съответствие с така възприетото от Съда на Европейския съюз, съдът в настоящия състав приема, че представените от ответника писмени доказателства налагат извод, че ответникът прилага мерки за защита на данните, съобразно задълженията му като администратор, уредени в ОРЗД и ЗЗЛД и в частност, сочените от ищцата чл.45, ал.1, т.6, чл.59, ал.11 чл. 64 от ЗЗЛД; чл. 66, ал.1 и ал.2, чл. 67 и чл. 68 от ЗЗЛД, съответно – че не е налице нарушение на §1, т. 10 от Допълнителните му разпоредби (ДР). Тези писмени доказателства безпротиворечиво установяват, че ответникът е прилагал трайно във времето, още от 2013г., широк обхват мерки за защита. Както е посочено в цитираното решение на Съда на Европейския съюз, обстоятелството, че въпреки тях е възникнало неразрешено разкриване на лични данни или неразрешен достъп до такива данни от трета страна не означава, че те не са били подходящи. Поради това, в случая не е налице първата предпоставка за ангажиране на отговорността на ответника.

Не се установи наличие и на втората предпоставка претърпяна вреда от страна на ищцата. Макар от приложената по делото справка от официалната страница на НАП да се установи изтичане на данни по отношение на нея, не бяха ангажирани доказателства за твърдените притеснения от разкриването им и възможна злоупотреба. За да бъде уважен искът по основание, следва по категоричен начин да се установи, че са настъпили претендираните от ищеца неимуществени вреди и, че те са в резултат на незаконосъобразното бездействие. Вредите, били те имуществени или неимуществени, не могат да са абстрактни и предполагаеми, а следва да са реално настъпили, съответно преживени. Недоказването на твърдените вреди, както и липсата на незаконосъобразно бездействие на ответника прави безпредметно разглеждането на третата предпоставка.

Предвид изложеното дотук, съдът в настоящия състав приема, че следва предявеният иск с правно основание чл.82 §1, вр. §2 от ОРЗД, за присъждане на обезщетение за неимуществени вреди, изразяващи се в притеснения, страх и опасения за възможна злоупотреба с личните ѝ данни, произлезли от неизпълнение на задължения на ответника за защита на тези данни, да бъде отхвърлен като неоснователен и недоказан. Поради отхвърляне на основния иск и акцесорният иск, по отношение на законната лихва върху присъдената сума, считано от 15.07.2019г. (датата на увреждането) до окончателното изплащане на сумата, следва да бъде отхвърлен.

С оглед изхода на спора и на основание чл.143, ал.3 АПК следва да бъде уважено искането на ответника за юрисконсултско възнаграждение. Размера на последното съдът определя на 100 лв. съгласно чл.24 от Наредбата за заплащането на правната помощ, издадена на основание чл.37, ал.1 от Закона за правната помощ.

Така мотивиран, съдът

РЕШИ:

ОТХВЪРЛЯ иска с правно основание чл.82 §1, вр. §2 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, предявен от Г. Д. Г., с ЕГН [ЕГН], против Националната агенция за приходите, за сумата 1000 (хиляда) лева, представляваща обезщетение за неимуществени вреди, ведно с лихвата върху тази сума, считано от 15.07.2019г. до окончателното ѝ изплащане.

ОСЪЖДА Г. Д. Г., с ЕГН [ЕГН], да заплати на Националната агенция за приходите сумата 100 (сто) лева - юрисконсултско възнаграждение.

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

Съдия: