Р Е Ш Е Н И Е
№ 7523

гр. София, 23.12.2020 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 48 състав,** в публично заседание на 07.12.2020 г. в следния състав:

СЪДИЯ: Калина Пецова

при участието на секретаря Евгения Стоичкова и при участието на прокурора Яни Костов, като разгледа дело номер **4773** по описа за **2020** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е образувано по Искова молба от А. П. М. от [населено място], обективираща иск, предявен срещу Националната Агенция по Приходите /НАП/за обезщетение за нанесени неимуществени вреди на ищцата, в размер на по 200 лв, предявен на осн. чл. 203 АПК вр. чл. 82 ал.1 от Общия регламент за защита на личните данни /ЕС/ 2016/679 на Европейския парламент и на Съвета от 27.04.16г / GDPR/, вр. чл. 39 ал.2 от ЗЗЛД вр. чл. 1 ал.1 от ЗОДОВ.

С исковата и уточнителната молба се сочи, както следва:

Претендират се 200 лева, представляващи обезщетение за претърпени неимуществени вреди от ищеца, причина за които е поведението на НАП или длъжностни лица при същия, изразяващи се в незаконосъобразно бездействие, вследствие от което е установено изтичане на личните данни на лицето от базата данни при ответника.

Сочи, че НАП , съгласно чл. 59, ал.1 от ЗЗЛД, като администратор на лични данни, е била длъжна, като отчита естеството, обхвата, контекста и целите на обработване, 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 със закона. Същото задължение следва и от чл. 24 от Общия регламент относно защитата на лични данни /ЕС/ 2016/679 на Европейския парламент и на съвета от 27.04.2016г. В чл. 32 от същия били предвидени конкретни мерки, които следва да бъдат взети при администрирането и обработването на лични данни , като тези задължения са въведени за да гарантират един от основните принципи за обработване на личните данни, прогласен в чл. 5, пар.1, б. „е“ от Регламента –

цялостност и поверителност на данните.
Счита, че в случая НАП не е положила достатъчна грижа и не е приложила ефективни мерки за защитата на сигурността на данните, с което не е изпълнила задължението си по чл. 24 и чл. 32 от Регламента, респ. чл. 59, ал.1 от ЗЗЛД.
Сочи, че обстоятелството, че е изтекла информация / конкретно име, презиме, фамилия и ЕГН, адрес и имуществено състояние /, вследствие на неоторизиран достъп до сървърите на НАП, сочи на противоправно поведение на ответника да изпълни произтичащите от закона задължения да защити физически лица във връзка с обработваните лични данни , тъй като именно техническата уязвимост на информационната система е довела до нерегламентираното разкриване и разпространение на лични данни, а тази уязвимост е вследствие от неприлагането на подходящи мерки за защина.
Вредите са неимуществени и се изразяват в чувство на безпокойство, паника, тревожност и психически дискомфорт.
Ответникът представя подробно писмено становище за недопустимост, алтернативно за неоснователност на жалбата.
В проведеното съдебно заседание ищецът се явява лично и се представлява от адв. О. с редовно пълномощно. Поддържат исковата претенция. Претендират разноските по производството. Представя подробни писмени бележки.
Ответникът се представлява от юрк Т. с редовно пълномощно. Оспорва исковата молба и моли същата да бъде оставена без уважение. Депозира подробни писмени бележки, като претендира юрисконсултско възнаграждение.
Представителят на СГП изразява становище за недоказаност и неоснователност на исковата молба.
Съдът, на база данните по делото, становищата на страните и въз основа на закона, намира исковата молба за недоказана и неоснователна.
За да стигне до този извод, съдът съобрази следното:
Производството е по реда на чл. 204, ал.4 от АПК във връзка с чл. 1, ал.1 от ЗОДОВ във връзка със ЗЗЛД.
Претендира се незаконосъобразно бездействие на ответната администрация, от което са причинени твърдените вреди в правната сфера на ищеца.
Процесът е исков, провежда се при диспозитивно начало на производството, което не изключва задължението на съда по чл. 170 от АПК за разпределяне на доказателствената тежест.
Дадени са указания от страна на съда за възможността да се ангажират доказателства, с оглед уточнение на иска, и в частност на това – кои конкретни технически, фактически, правни действия на кои длъжностни лица при ответника са извършени, респ. не са извършени, така, че последното е довело до изтичането на данни, довели до претендираните вреди.
Постъпила е уточнителна молба от адв. О. от 29.06.2020г., в която излага съображения, че обстоятелството, че е изтекла информация / конкретно име, презиме, фамилия и ЕГН, адрес и имуществено състояние /, вследствие на неоторизиран достъп до сървърите на НАП, сочи на противоправно поведение на ответника да изпълни произтичащите от закона задължения да защити физически лица във връзка с обработваните лични данни , тъй като именно техническата уязвимост на информационната система е довела до нерегламентираното разкриване и разпространение на лични данни, а тази уязвимост е вследствие от неприлагането на

подходящи мерки за защина.
Фактическият състав на чл.1, ал.1 от ЗОДОВ включва установяване на неправомерно деяние, което е предизвикало конкретни вреди – материални или нематериални в правната сфера на ищеца, както и причинно-следствената връзка между тях.
Съдът отбелязва, че доказателствената тежест по делото, доколкото се касае за исково производството , е разписана в чл.1, ал.2 от ЗОДОВ във връзка с чл. 203 и следващи от АПК, както и е указана с определението за насрочване на делото от 15.11.2019г. – „Страните могат да сочат доказателства, като ищецът носи доказателствена тежест да установи фактите, включени във фактически състав на нормата на чл.1, ал.1 от ЗОДОВ, а именно – незаконосъобразно действие/бездействие от страна на административния орган или служител при същия, вреда в правната му сфера, причинно-следствена връзка между тях.“
Съдът намира, че първата предпоставка от фактическия състав на чл.1, ал.1 от ЗОДОВ остава недоказана по делото от страна на ищеца, въпреки указаната му възможност да ангажира доказателства в тази насока.
Посоченото от ищеца поведение, което следва да представлява незаконосъобразното бездействие е „ НАП не е положила достатъчна грижа и не е приложила ефективни мерки за защитата на сигурността на данните , с което не изпълнила задълженията си по чл. 24 и чл. 32 от Регламента и чл. 59, ал.1 от ЗЗЛД. Твърдят се още нарушения на чл. 45, ал.1, т.6 от ЗЗЛД; чл. 64 от ЗЗЛД; чл. 66, ал.1 и ал.2 от ЗЗЛД; чл. 67 от ЗЗЛД; чл. 68 от ЗЗЛД, като изброените са довели до нарушение по §1, т.1 0 от ДР на ЗЗЛД във връзка с чл. 4, т. 12 от Регламента.“
Съдът приема, че в обхвата на доказване следва да бъде установено конкретно деяние, което да представлява неправомерно бездействие от страна на администрацията на НАП, което именно да е довело до безспорния резултат – изтичане на лични данни от базата данни, чийто администратор е НАП. Твърди се нарушение, което винаги представлява конкретно деяние – действие или за процесния случай – бездействие. Фактическият състав по доказването му включва установяване на конкретно фактическо, техническо или правно дължимо действие, което не е извършено при възникване на предпоставките за извършването му.
Съдът приема, че следва да бъде изследвано наличието на конкретно действие от страна на отговорните служители за това при ответника, което им е било вменено, но същите не са го изпълнили изобщо, или некачествено, или извън срока, предвиден за това. Следва да бъде изследвана и хипотезата, при която е следвало да бъде въведена конкретна система, софтуер, методика или какъвто и да е друг технически способ, въведен чрез вътрешнослужебните актове на органа или по нормативен път, което да е било задължително с цел избягване на установеното изтичане, което да не е било сторено изобщо, или некачествено, или извън срока.
Иначе казано, т. наречените „подходящи и ефективни мерки организационни и технически мерки “ следва да бъдат установени чрез изследване наличието задължения за администрацията, които са останали неизпълнени или лошо / некачествено или късно/ изпълнени или задължения на служители при администрацията на НАП, които да не са изпълнени, или лошо / некачествено или късно/ изпълнени.
Разпространената на 15.07.2019г. информация чрез медиите за установен неоторизиран достъп до обработваните от НАП бази данни с лични данни / ЕГН, име/ е безспорно установен факт. Последното е вследствие на хакерска атака, като е

образувано и досъдебно производство по случая за киберпрестъпление, за което към момента на приключване на съдебното дирене, няма данни да е приключило.
Касае се за противоправно поведение от страна на трети неустановени лица, което е довело до негативния резултат – неоторизиран достъп. Т.е., предмет на евентуалното престъпление по досъдебното производство е именно посегателство върху обработваните от НАП бази данни с лични данни, което представлява интелектуална собственост. Срещу същата е налице противоправно посегателство от трети лица. Липсва каквато и да е презумпция за противорправно поведение /включително действие/ бездействие/ на собственика на базата данни, в случая администратора на лични данни – НАП, което да е довело или да е съпричинило за така установеното деяние. Обратното би означавало, че всеки субект, срещу когото е реализирано посегателство, следва да понесе отговорност, че е допуснал същото, поради наличие на негово противоправно поведение.
Именно поради това, съдът намира, че в тежест на ищац е да посочи кои са тези конкретни деяния / реализирани чрез фактически, технически или правни действия/, които е следвало да извърши НАП или длъжностни лица при нея, но не ги е извършила или ги е извършила лошо, така че да е допринесено за противоправния резултат – неоторизиран достъп.
Такива не бяха посочени с цел установяване и доказване. Тезата относно незаконосъобразното бездействие се гради на установения противоправен резултат – неоторизирано изтичане на данни, от където се презумира, че е налице противоправно бездействие, довело до същия.
Съдът възприема тезата, че установеният вредоносен резултат /установен неоторизиран достъп/ не доказва сам по себе си деянието от страна на извършителя му / което е предмет на висящо досъдебно производство/, а още по-малко наличие на противоправно поведение у пострадалия, който в случая е собственика на базата данни – НАП и администратор на личните данни, съхранявани в същата.
Съдът, по изложените по-горе мотиви, не възприема тази теза, поради което счита, че само на това основание, първата предпоставка на фактическия състав по чл.1, ал.1 от ЗОДОВ, се явява недоказана. Липсват изобщо конкретни твърдения за деяния, представляващи твърдяното бездействие, които да бъдат предмет на установяване и проверка в производството.
Въпреки това и за пълнота, на база приетите по делото доказателства, съдът намира, че такива деяния не се доказаха.
От представените писмени доказателства се установява следното за организацията на опериране с базите данни от страна на НАП.
По отношение функционирането на електронните услуги на НАП, са разработени и осигурени технически процедури по идентификация на потребителите с електронен подпис, персонален идентификационен код, издаван от НАП, както и CAPTCHA / тест за сигурност за разграничаване на компютри от хора/.
В НАП има действаща процедура ИС 17, версия В, „Администриране на информационната система в НАП“, утвърдена със Заповед №ЗЦУ-1236/21.08.2019г. На Изпълнителния директор на НАП, с която е отменена действащата до този момент Процедура ИС17 , утвърдена със Заповед №ЗЦУ-1767/29.12.2017г. на Изпълнителния директор на НАП. Същата е съобразена във всичките й версии с изискванията, регламентирани в Наредба за общите изисквания за оперативна съвместимост и информационна сигурност и Наредба за минималните изисквания за мрежова и

информационна сигурност /ДВ, бр. 59 от 26.07.2019г./
В изпълнение на цитираните нормативни актове, е извършено тестване със специализирано техническо средство Qualys, предназначено за мониторинг и идентифициране на уязвимости в информационните активи.
НАП има най – голям брой електронни услуги в цялата администрация – 138 броя, които са създадени и поддържани в изпълнение на държавната политика за намаляване на административната тежест и предоставяне на качествени , ефективни и леснодостъпни онлайн услуги за гражданите и бизнеса.
Целите на електронното управление, определени в Стратегията за развитие на електронно управление в Република България 2014г. - 2020г. , както и действащата нормативна рамка , са насочени към внедряването, развитието и употребата на електронни административни услуги. НАП е предприела в тази насока всички необходими технически и организационни мерки, за да минимизира рисковете от поддържането на такъв голям обем електронни услуги. Рисковете не могат да бъдат на 100 % процента , а избегнати, а задължението се свежда до предприемане на мерки за минимизацията им. Въпреки тях е реализирано киберпрестъпление.
Доказва се, че в края на 2018г. е извършена проверка на НАП от Държавна агенция „Електронно управление“ с обхват изпълнение на изискванията, предвидени в Закона за електронно управление, Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги и Наредбата за общите изисквания за мрежова информационна сигурност. Проверката не е констатирала нарушения и/ или неизпълнение на нормативни задължения, предвидени в цитираните нормативни актове.
В НАП са разработени:
– Политика по защита на личните данни, утвърдена със Заповед № ЗЦУ-746 от 25.05.2018г. На Изпълнителния директор на НАП;
– Заповед № ЗЦУ-1595/29.11.2017г. На Изпълнителния директор на НАП за утвърждаване на указания за обозначаване и работа с информацията, ведно с Указания и обозначаване за работа с информацията, версия3.0;
– Политика по информационната сигурност на НАП, версия 3.0, май 2016г.;
– Инструкция №2/08.05.2019г. За мерките и средствата за защита на лични данни, обработвани в НАП и реда за движение на преписки и заявяване на регистри, ведно с Декларация за опазване на лични данни, която се подписва от всички служители на НАП;
– Заповед № 586 от 30.04.2014г. за внедряване на система за управление на сигурността на информацията;
– Методика за оценка на риска, версия 1, декември, 2013г.
След оповестяване и узнаване за неоторизирания достъп, на основание чл.22 от Регламента, НАП незабавно уведомява за случая КЗЛД с писмо, изх. № ЕП-37-00-137 от 16.07.2019г,. приложено по делото.
Уведомена е и Софийска градска прокуратура с писмо, изх. № 11—02-231/17.07.2019г. - за наличие на данни за извършено престъпление чрез осъществен неоторизиран достъп до информационната система на НАП и разпространение на защитена информация на граждани, обработвани от Агенцията, с искане за незабавно образуване на наказателно производство по случая. Уведомени са специализираните звена при ГД „БОП“, в МВР и ДАНС.

Предприети са мерки за незабавно уведомяване на обществеността чрез онлайн и други медии, както и са предприети мерки за преустановяване на нерегламентирания достъп.

За теча на данни е докладвано на секретариата на Глобалния форум за прозрачност и обмен на информация за данъчни цели / Глобален форум/ към Организацията за икономическо сътрудническо и развитие. Незабавно са предприети мерки за справяне с нарушения на сигурността на данните с действително или потенциално въздействие върху данните , обменяни с международни партньори за обмен на информация за данъчни цели. На 28-30.08.2019г. екип от експерти от Глобалния форум извършва проверка относно установения нерегламентиран достъп и установява следното: - Всички информационни системи на НАП, вкл. услугите, предоставяни на клиенти, са прегледани за уязвимост;

– Всички услуги онлайн и съответните приложения са проверени за уязвимост и тези с потенциална такава са били спрени;

– Извършена е проверка на изходния код на всички приложения, които са разработени или вътрешно от НАП, или от външни изпълнители;

– Конфигурацията на мрежите и приложните сървъри е проверена и актуализирана;

– Правата на достъп до схемите в базата данни са преразгледани и актуализирани;

– Създадена е нова среда за изпитване, с цел симулация на атаки и тестване на уязвимостите на приложенията;

– Грешките, свързани с изходния код на приложенията са проактивно поправяни;

– Преразгледани са всички пароли, вкл. тези на администраторските профили и на сервизните профили;

– Преразгледани са всички права на привилегировани потребите.

Установено е, че действащите до момента в НАП процедури, които се отнасят до сигурността на информацията, са напълно адекватни и отговарят на изискванията: Искане за предоставяне на нови или промени в съществуващите информационни системи, интерфейси РР, бази данни, хардуерни устройства или други информационни активи, оценка и вземане на решение за тяхната покупка/ разработване; Изготвяне на подробни изисквания за закупуване/ разработване на нови или промени в съществуващите информационни системи или програмни продукти; Проектиране на информационни системи; Разработване на информационни системи; Тестове и приемане на разработени или предоставени информационни системи или програмни продукти; извършване на контрол за спазване на изискванията на системата за управление на информационната сигурност; Оценка на риска във връзка с информационната сигурност.

След установяване на инцидента са предприети следните конкретни мерки, извън извършеното уведомяване:

– Установени са по-конкретни и стриктни правила за достъп;

– Стартира процес по конфигуриране на приложна защитна стена, която да идентифицира и блокира опити за експлоатиране на уязвимости приложения на НАП;
– Реализиран е допълнителен защитен слой на публичният сайт на НАП, чрез конфигурирането му по начин, позволяващ да използва анти-D. доставчик С.. През този канал минава единствено и изцяло публична информация, начална на Интернет страницата на НАП, тъй като продължават атаките срещу публичните ресурси на НАП;
– Извършена се наблюдение на логовете на приложенията и системите, внедряват се системи и процесиза централизираното им наблюдение с цел подобряване на нивото на регистриране на потребителските действия;
– Създадени са потребители с административни права в активната директория на НАП, с цел следене на опити за достъп, пуснат е процес на логване на действията, проследяване и нотификация в реално време при опити за използването им;
– Преконфигурирани са връзките на сървърите на базите данни и приложенията, което е довело до увеличаване на бързината и ефективността на информационните системи. Архивите на базите данни се намират на устройства за съхранение на данни, което гарантира запазването им;
– Внедрен е процес на периодично архивиране на състоянието на приложните сървъри на критичните ИС, с цел възстановяването им при атака или срив. На някои системи е извършена миграция на по-високи версии на приложна среда, което ограничава повърхността за атака срещу базовите компонентни на тези системи;
– На самостоятелен физически сървър, до който няма достъп външното пространство са мигрирани данните от международния обмен на информация.
– Проведено е специализирано обучение по спазване на правилата за сигурност, заложени в Наредбата за минималните изисквания за мрежова и информационна сигурност.
– Извършен е пълен преглед на всички приложения в информационните системи на НАП- от кои служители се ползват и доколко е целесъобразно това.

Продължават да се изпълняват следните дейности:

– Преразглежда се архитектурата на базата данни, с цел преместване на ненужните данни и архивиране на информацията, която е остаряла и ще се ползва рядко;
– Разработва се план за актуализация на версията на

криптографските протоколи, които осигуряват сигурността на комуникацията;

– Анализира се възможност за реализиране на двуфакторна идентификация на служителите на НАП и на администраторите;

– Проведено е обучение на служителите от дирекция „Информационни системи и моделиране на бизнес процесите“ за сигурно програмиране и проверка на сигурността по време на разработката.

Последните данни са видни от изложението на ответника, като съдът ги излага само за пълнота, тъй като по делото няма яснота дали поддръжката на базата данни преди неоторизирания достъп, и съответно иновациите , въведени след това, са довели, респ. биха предотвратили възможността той да бъде реализиран.

Конкретни твърдения в тази насока не са правени, респ. не са ангажирани доказателства.

Т.е., при реализиране на някоя от предпоставките на хипотезата, без значение дали неправомерно или случайно, е налице нарушаване на сигурността на обработваните данни. Причините и евентуалната вина за това / неправомерно или случайно и по какви причини/ подлежи на доказване. Последното следва от логическото тълкуване на чл. 32, §3 от Регламента, който предписва способи /приложение в чл. 40 и чл. 42 от Регламента/ с цел доказване на мерките, предписани за спазване в §1 от същата разпоредба. Последната предвижда препоръчително извършването на определени операции от администраторите, с цел опазване на сигурността. При установено нарушаване на тази сигурност, на администратора е предоставена нарочна възможност да се защити, вкл. чрез конкретни насоки, ерго от установеното нарушаване на сигурността на данните, не следва автоматично, че е налице нарушение, осъществено от администратора на данните.

В процесния случай са спазени разпоредбите на чл. 33 и чл. 34 от Регламента, като е проведено предписаното в тях уведомяване.

Чл. 45, ал.1, т. 6 от ЗЗЛ предвижда, че личните данни следва да се обработват по начин, който гарантира подходящо ниво на сигурност, като се прилагат подходящи технологии и организационни мерки.

Съдът за пореден отбелязва, че за нуждите на настоящото производство и към момента на приключване на съдебното дирене, са установени множество организационни мерки за внедряване на съответни технологии от страна на НАП за поддържане на базата данни при същата, вкл. съдържаща и лични данни. Към същия момент и в същото производство не се установи обратното – прилагане на неподходящи технологии или липса на организационни мерки. Отново съдът намира, че

следва да посочи, че осъщественият резултат – нерегламентиран достъп не е еднозначно следствие и не доказва причината за себе си. За нуждите на делото бе нужно да бъде доказано обратното – наличието на несъответни организационни мерки, респ. технологии.

Чл. 64 от ЗЗЛД задължава администраторите на лични данни да извършват оценка на въздействието на предвидените операции по обработване на личните данни върху тяхната защита. С политика по информационна сигурност на НАП, версия 3.0 от май, 2016г. /л.74-86 по делото/, такава оценка е въведена, както превантивно, така и с непрекъснат мониторинг и оценяване на процеса – т. 7 и т. 8 от Политиката.

Чл. 66, ал.1 и ал.2 от ЗЗЛД възпроизвежда текста на чл. 32 от Регламента, по който въпрос съдът вече взе отношение. От приложените и изброени документи, цитирани на лист 7 в настоящото решение е видно, че органът е предприел мерки с оглед опазване на личните данни, които обработва, като са съобразени всички действащи нормативи и предписани с тях задължения , съобразени с техническия прогрес и разходите за прилагането им.

Нормите на чл. 67 и чл. 68 от ЗЗЛД възпроизвеждат относно норми на Регламента, като същите не са нарушени, поради установено безспорно уведомяване както на компетентните органи – КЗЛД, Прокуратура и МВР, така и на обществеността.

По изложените съображения , съдът категорично приема, че по делото не се установява първата предпоставка от фактическия състав на иск по чл.1, ал.1 от ЗОДОВ – установено незаконосъобразно бездействие, довело до твърдяното увреждане, предмет на претенцията.

Последното е достатъчно за отхвърляне на исковата молба като недоказана и неоснователна, но за пълнота съдът намира, че следва да отбележи още, че споделя тезата на процесуалния представител на ответника, че не се доказа настоящият ищец да е предприел действия за установяване на това – кои конкретни лични негови данни са били предмет на посегателство, въпреки организираната възможност за това. Последното внася съмнение в степента на тревожност и ангажираност, която е създадена у него от изтичането на информацията. Поради което изложените притеснения , дори и да бяха доказани, не биха били в причинно-следствена връзка с установения неоторизиран достъп до личните данни на НАП.

По изложените съображения, съдът намира, че следва да остави исковата молба като недоказана и неоснователна.

При този изход на спора, в полза на ответника следва да бъде

присъдено претендираното юрисконсултско възнаграждение в размер от 100 лева, по аргумент от чл. 10 , ал. 4 от ЗОДОВ във връзка с чл.37 от Закона за правната помощ и чл. 25, ал.1 от Наредбата за заплащането на правната помощ.

Воден от горното и на основание чл. 203 и сл. от АПК във връзка с чл.1, ал.1 от ЗОДОВ, съдът

РЕШИ:

ОСТАВЯ БЕЗ УВАЖЕНИЕ исковата молба от А. П. М. от [населено място], обективираща иск, предявен срещу Националната Агенция по Приходите /НАП/за обезщетение за нанесени неимуществени вреди на ищцата, в размер на по 200 лв, предявен на осн. чл. 203 АПК вр. чл. 82 ал.1 от Общия регламент за защита на личните данни /ЕС/ 2016/679 на Европейския парламент и на Съвета от 27.04.16г / GDPR/, вр. чл. 39 ал.2 от ЗЗЛД вр. чл. 1 ал.1 от ЗОДОВ.

ОСЪЖДА А. П. М. да заплати в полза на НАП сумата от 100 / сто/ лева, представляваща претендираното юрисконсултско възнаграждение.

Решението подлежи на оспорване в 14-дневен срок от връчването му на страните пред ВАС.

Преписи от решението да се изпратят на страните.

СЪДИЯ: