Р Е Ш Е Н И Е
№ 7207

гр. София, 11.12.2020 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 39 състав,** в публично заседание на 23.09.2020 г. в следния състав:

СЪДИЯ: Миглена Николова

при участието на секретаря Александра Вълкова и при участието на прокурора Десислава Кайнакчиева, като разгледа дело номер **10466** по описа за **2019** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 203 и сл. от АПК.

Образувано е по Искова молба вх.№ 27810/16.09.19г на Е. А. Г. от [населено място] и с проц.представител адв. С.Ю., с която е предявен Иск по чл. 39 ал.2 от ЗЗЛД 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/ против администратор на лични данни - НАП, с цена на иска 1000лв, представляващи обезщетение за причинените неимуществени вреди от незаконосъобразно фактическо бездействие на НАП да изпълни задълженията си по чл. 24 и чл. 32 от Регламента и по чл. 45 ал.1 т.6, чл. 59 ал.1, чл. 64, чл. 66 ал.1 и ал.2, чл. 67 и чл. 68 от ЗЗЛД, довело до нарушение на сигурността на личните данни по см. на § 1 т.10 от ДР на ЗЗЛД вр. чл. 4 т.12 от Регламент 2016/679 и допуснат пробив в информационната система на НАП с резултат- публично разгласяване на личните данни на около 5 000 000 български граждани /граждани на ЕС/, станало публично известно чрез медиите на 15.07.19г.Претендира се и законна лихва, считано от 15.07.19г или алтернативно-от 16.09.19г/датата на ИМ/, до окончателното изплащане на сумата.

В ИМ ищецът сочи, че НАП е администратор на лични данни съгл. чл. 4 т.7 от Регламента, като съгл. чл. 59 ал.1 от ЗЗЛД е длъжен да вземе подходящите технически и организационни мерки, за да гарантира, че обработването на личните данни се извършва в съответствие с изискванията на ЗЗЛД.Същото задължение администраторът има и по чл. 24 от Регламента, като в чл. 32 от Регламента са

разписани конкретните мерки, които следва да се вземат от администратора при администрирането и обработването на лични данни, за да се гарантира основния принцип по чл. 5 §1 б.“е“ от Регламента- за цялостност и поверителност на данните.На 15.07.19г от медиите става публично известно, че чрез т.нар. „хакерска атака“ от електронните масиви на НАП е изтеглена неправомерно голям обем информация, съдържащи личните данни на около 5 000 000 български граждани.НАП е държавен орган, който отговаря за приходите на държавата, без които тя изобщо не би могла да функционира.Поради което би следвало НАП да е обезпечила по безупречен начин своята кибер-сигурност, респ. в най-голяма степен да гарантира по ефективен начин и сигурността на личните данни на гражданите на РБ.НАП не е изпълнила това свое задължение в най-добра степен, като е налице неполагане на достатъчна грижа и неприлагане на ефективни мерки за защита на личните данни.Ищецът е получил информация чрез специално разработеното приложение на НАП, че и негови лични данни са изтекли при пробива/което не се оспорва от ответника/. В резултат на което ищецът е понесъл неимуществени вреди , изразяващи се в силно притеснение, че с личните му данни ще бъде злоупотребено /възможно е да се отчужди имуществото му, да бъдат изтеглени влоговете му, да бъдат изтеглени кредити на негово име, да бъде променено гражданското му състояние, да бъде откраднатa самоличността му, да бъдат използвани по всевъзможни начини личните му данни, за да му се навреди/.Според публикации в медиите, специалистите намират случая за много сериозен, като дори не се знае кога и как точно ще се злоупотреби с изтеклите лични данни. Ищецът се чувства много натоварен психически, както и възмутен от огромния брой засегнати бълг.граждани. От 15.07.19г/деня на пробива/, ищецът живее в постоянен страх и притеснение, чувства се незащитен от държавата, изключително напрегнат, стресиран и уплашен.Налице е страх и от физически нападения, заплахи,изнудвания и отвличания, поради изтеклите данни за доходите и адреса.Още преди 15.07.19г, КЗЛД е дала указания на НАП за въвеждане на втори идентификатор/освен ЕГН/, като НАП е избрала за такъв- първите 6 цифри от ЕГНто, т.е вторият припокрива първия идентификатор и така не се осигурява никаква по-сериозна защита на личните данни.От 2008г не е правено осигуряване на сървъра и осигурителните системи на НАП, не е осигурен резервен сървър, като не са предприети никакви мерки за гарантиране сигурността на личните данни . Външни лица влизат в сървъра на НАП чрез потребителско име и парола на един термин-admin /явно сигурността на информацията не е приоритет, щом не се ползва парола за защита от 12 символа-цифри и букви/.Поне 3 държави /Германия, Б. и С./, спират обмена на чувствителна дан.информация с РБ, тъй като намират инцидента за сериозен /а РБ е част от межд.мрежа за автоматична размяна на дан.информация, създадена да противодейства на укриване на бюджетни задължения и пране на пари/. НАП е нарушила посочените норми на ЗЗЛД , съгл. които: личните данни се обработват по начин, гарантиращ подходящо ниво на сигурност, като се прилагат подходящи технологии и организационни мерки; извършване на оценка на въздействието на предвидените операции по обработване на личните данни върху тяхната защита; прилагане на подходящи техн. и организационни мерки за осигуряване с този риск ниво на сигурност, като се отчитат достиженията на техн.прогрес, разходите за прилагане, естеството,обхвата,контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица; в случаите на нарушение на сигурността на личните данни, което има вероятност да

доведе до риск за правата и свободите на субектите на данните, администраторът не по-късно от 72 часа след като е разбрал за нарушението, следва да уведоми КЗЛД; когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на субектите на данните, администраторът следва да уведоми субектите на данните за нарушението не по-късно от 7 дни от установяването му-с писмено уведомление. Описаните нарушения на НАП са довели до „Нарушение на сигурността на личните данни“ по см. на §1 т.10 от ДР на ЗЗЛД вр. чл. 4 т.12 от Регламента /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/.Налице е пряка причинно-следствена връзка между нарушенията на НАП и претендираните вреди, като предвид чл. 39 ал.2 от ЗЗЛД вр. чл. 82 ал.1 от Регламента, НАП /която е и държавен орган/ следва да носи отговорност за вредите на осн. чл. 1 ал.1 от ЗОДОВ, по реда на чл. 203 и сл. от АПК.В уточняваща искова молба се сочи, че е налице обективна отговорност на адм.орган, който носи отговорност по чл. 1 ал.1 от ЗОДОВ ,като е ирелевантно дали конкретно длъжностно лице от структурата на НАП е действало виновно.Отново се сочи, че НАП е бездействала, като не е положила от една страна- достатъчно грижа, а от друга страна- ефективни мерки, така че да защити сигурността на данните.В съд.заседание адв. Ю. поддържа иска, като сочи, че от представените доказателства от НАП не се установяват предприети от администратора реални фактически действия по осигуряване защитата на личните данни, а само наличие на предписания за извършване на такива действия.Всички твърдения от ИМ са доказани от материалите по делото, поради което се моли за уважаване на иска в цялост.Моли се за присъждане на разноски по списък, вкл. 30лв за частната жалба пред ВАС.

Ответникът Национална Агенция по приходите чрез проц.представител юрк. Т. в отговора си оспорва иска като недопустим и рес. неоснователен и недоказан, като сочи, че НАП е узнала за теча на данни на 15.07.19г, но все още не е известно кога е направен пробива в системата й.НАП е разработила специално приложение, чрез което всеки гражданин може да направи справка дали негови лични данни са изтекли при пробива.Ищецът е научил, че негови лични данни са изтекли чрез справка в това приложение - на 03.08.19г. Изтеклите лични данни на ищеца са : ЕГН. Нерегламентираният достъп е до база данни на НАП, а не до конкретни документи на ФЛ.Сочи се, че до момента няма влезли в сила адм. или съд.актове, потвърждаващи, че нерегламентираният достъп се дължи на действия/актове/бездействия на НАП или нейни служители, тъй като пробивът е в резултат на престъпление по НПК /действие без оглед на предприетите мерки за сигурност и въпреки тях/. В НАП са въведени и функционират Система за управление на бизнес процесите и Система за управление на сигурността на информацията, като всички процедури в НАП/утвърждавани съгл. чл. 10 ал.1 т.5 от ЗНАП/ са съобразени с межд.стандарти за управление на качеството като ISO 9000 и ISO 9001.В НАП се обработва голям обем от данни, представляващи защитена по закон информация, поради което за тях се прилагат утвърдени и действащи политики,правила,процедури,инструкции,указания и методики за управление на сигурността на информацията.Вътрешните документи относно информационната сигурност се утвърждават от ИД на НАП и са съобразени със Закона за електронното управление, Наредбата за общите изисквания към инф.системи, регистрите и електронните адм.услуги и наредбата за общите

изисквания за мрежова и информационна сигурност.Правилата и процедурите в НАП относно обработването на лични данни са задължителни за всички служители на НАП, като в утвърденото от ИД на НАП-Указание за обозначаване и работа с информация е предвидено информацията, съдържаща лични данни да се маркира с „ограничено ползване“ и са предвидени орган. и техн.мерки за работа с нея.Веднага след като е научила за пробива/на 15.07.19г/, НАП е предприела действия за уведомяване на КЗЛД,СГП, ГДБОП, ДАНС, засегнатите ФЛ и партньорите.НАП е станала обект на злоумишлено посегателство и не следва тя да носи отговорност за вреди от престъпление, като НАП е била предприела към 15.07.19г необходимите техн. и организационни мерки. След 15.07.19г НАП е провела поредица от срещи с представители на множество институции в РБ, на които са обсъдени рисковете изтеклите лични данни да бъдат неправомерно използвани и от които става ясно, че няма непосредствена такава опасност.НАП многократно публично е успокоявала гражданите, че няма опасност за тяхното имущество, като на сайта й има разработени специални рубрики с най-често задаваните въпроси от потърпевшите и е публикуван кратък информационен видеофилм със съвети към гражданите.Разработено е приложение и електронна услуга, чрез които всеки да може да провери дали и неговите лични данни са сред изтеклите такива.Целта на всички тези действия на НАП е да се преодолее неоснователното според нея безпокойство у гражданите за евентуални злоупотреби с техните лични данни/вкл. изтеклата данъчна и осигурителна информация за тях/.Ответникът счита, че тъй като не е налице доказано /с влязъл в сила акт/ незаконосъобразно бездействие или действие на НАП или негови служители, не е налице първата предпоставка за основателен иск по чл. 1 ал.1 от ЗОДОВ. В допълнение, не е доказана и причинно-следствената връзка между претендираните вреди и недоказаната първа предпоставка за основателност на иска.Моли се за прекратяване на производството поради недопустимост на иска, респ. за отхвърляне на иска изцяло като неоснователен и недоказан и присъждане на юрисконсултско възнаграждение. В доп.становище НАП сочи, че обекти на внедрената Система за управление сигурността на информацията са : всички данни в инф.системи на НАП, системната информация, техн.средства, системен и приложен софтуер, електронни и хартиени носители на информацията, сгради, сигурни помещения/сървърни,архивни помещения/. Защитата на информацията се осъществява на всеки етап от инф.процес- създаване,обработка,съхранение,пренасяне и унищожаване, във всички структури на НАП.От момента на създаване на инф.системи на НАП съществуват системи за одитиране действията на потребителите. Всички данни в системите и услугите на НАП се разглеждат като инф.актив, който се идентифицира,класифицира,оценява,превентира и управлява съгл. одобрената Методика за оценка на риска и процедура за оценка на риска/в утвърдени форми са идентифицирани заплахите и способите за оценка на риска/, в съответствие с установената Политика за управление на риска/т.7 на Политика на инф.сигурност в НАП/.Оценка на риска в НАП се извършва при първоначалното въвеждане в експлоатация на нови системи, при промяна на системите, периодично/организирано от звеното по мрежова и инф.сигурност/.Твърди се, че НАП като администратор на лични данни е изпълнила в достатъчна степен задълженията си по ЗЗЛД и Регламента. В съд.заседание юрк. Т. оспорва иска, по аргументи от депозирания отговор по иска.Сочи се, че и до момента/16.09.20г/ няма констатиран нито един случай на злоупотреба с изтеклите лични данни, нападения,заплаха,изнудване или

отвличане на гражданин с изтекли данни. Поради което страховете на ищеца са от предполагаеми събития, каквито не са се проявили.
Прокурорът изразява становище за неоснователност и недоказаност на иска, поради което същият следва да се отхвърли.
Според Определение № 5212/30.04.20г на ВАС, Искът е редовен и допустим и следва да се разгледа по реда на чл. 203 и сл. от АПК, а за неуредените въпроси- по реда на ЗОДОВ. ВАС е дал правната квалификация на Иска. Искът е предявен по местоувреда/, поради което съгл. чл. 7 от ЗОДОВ, АССГ е надлежния съд.
Съдът установи от фактическа страна следното:
Общоизвестно е , т.е. ненуждаещо се от доказване съгл. чл. 155 от ГПК, че на 15.07.19г в медиите в РБ се публикува информация, че чрез т.нар. „хакерска атака“ от електронните масиви на НАП е изтеглена неправомерно голям обем информация, съдържащи личните данни на около 5 000 000 български граждани.На същата дата и НАП научава за пробива, като и до момента не е известна датата, на която е станал пробива. На 25.07.19г ищецът прави справка на специално разработеното за целта приложение от НАП, като от справката на 03.18.19г /по ЕГН/ научава, че са изтекли и негови лични данни.Видно от представената от ответника справка, изтеклите лични данни на ищеца са: ЕГН.
В изпълнение указанията на Съда /че НАП носи доказ.тежест относно изпълнението, и то в достатъчна степен, на задълженията й като администратор по ЗЗЛД и по Регламента/, НАП представя : 1 / доказателства какви действия е предприела след 15.07.19г: На 16.07.19г НАП уведомява КЗЛД за случая, а на 17.07.19г НАП уведомява СГП за случая.На 17.07.19г започва пълен одит на инф.системи на НАП от независима външна организация с участието на ИТ екипа на приходната администрация.От 22.07 до 15.08.19г КЗЛД извършва проверка, образувано е досъдебно производство в СП.На 26.09.19г има изслушване на Прокуратурата на РБ пред Временна анкетна комисия на НС за изясняване на фактите и обстоятелствата около случая.На 10.10.19г такова изслушване има и по отношение на представители на Нотариалната камара, К. на частните съдебни изпълнители и Висшия адвокатски съвет; 2/ Методика за анонимизиране на индивидуални данни /версия 1, към м.01.17г; 3/Политика по инф.сигурност на НАП/версия 3.0 от м.05.16г/; 4/ Методика за оценка на риска /версия 1.1, към м.11.15г/; 5/ Инструкция № 2/08.05.19г за мерките и средствата за защита на лични данни, обработвани в НАП и реда за движение на преписки и заявяване на регистри /издадена от ИД на НАП, на осн. чл. 59 и сл. от ЗЗЛД и задължителна за всички органи и служители в НАП/; 6/ Заповед № З-ЦУ-1436/15.10.18г на ИД на НАП , издадена на осн. чл. 25 ал.1 вр. чл. 26 ал.2 от Наредбата за общите изисквания за мрежова и инф.сигурност , за постигане на мерките съгл. Политиката по инф.сигурност на НАП /утвърждават се Указания за разработване,попълване и/или зареждане с данни на образци на документи и приложения, Указания за обозначаване и работа с информацията, Указания за попълване на образеца на процедура, Указания за попълване на образеца на инструкция/; 7/ Заповед № ЗЦУ-746/25.05.18г на ИД на НАП за утвърждаване на Политика за защита на личните данни в НАП; 8/ Политика за защита на личните данни в НАП; 9/ Процедура за оценка на риска за информационната сигурност; 10/ Заповед № ЗЦУ-586/30.04.14г за внедряване, считано от 01.05.14г, на Система за управление на сигурността на информацията; 11/ Указания за обозначаване и работа с информацията /версия 3.1, към 2018г/; 12/ писмо от КЗЛД до НАП от 13.08.19г /в

отговор на запитване от 09.08.19г на НАП относно приложението на чл. 34 от Регламента и чл. 68 от ЗЗЛД/; 13/ Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействието върху защитата на данните съгл. чл. 35 §4 от Регламента.

Видно от отговор на КЗЛД на запитване на Съда : 1/ пред КЗЛД няма висящо или приключило производство по жалба на ищеца/във вр. чл. 39 ал.4 от ЗЗЛД/; 2/ при проверка на КЗЛД е установено, че са изтекли лични данни на 6 074 140 физически лица, от които 4 104 786 живи български и чужди граждани и 1 959 598 починали ФЛ; 3/ изтеклите данни на ФЛ са **имена,ЕГН, адреси, телефони, ел.адреси, данни от годишни дан.декларации на ФЛ, данни от справките за изплатени доходи на ФЛ, данни от осигурителните декларации, данни за здравноосигурителни вноски,данни за издадени АУАН, данни за извършени плащания на данъци и осигурителни задължения през [фирма], данни за поискан и възстановен ДДС-платен в чужбина**; 4/ На НАП е издадено от Председателя на КЗЛД - НП № 004/28.08.19г , за нарушение на чл. 32 §1 б.“б“ от Регламента, което е предмет на висящо съд.производство пред СРС; 5/ С Решение № ППН-02-399/22.08.19г КЗЛД дава на НАП разпореждане по чл. 58 §2 б.“г“ вр. чл. 57 §1 б.“а“ и чл. 83 §2 б.“а“,б.“в“, б.“г“, б.“е“ и б.“ж“ от Регламента за предприемане на подходящи техн. и организационни мерки за защита на личните данни,предмет на висящото адм.дело № 10477/19г на АССГ.

Относно вредите, Съдът е разпитал свид.Н./живее на съпружески начала с ищеца, води аналогично дело срещу НАП/. Свидетелката твърди, че когато ищецът научил от получения в отговор на запитването му СМС от приложението на НАП, че и негови лични данни са изтекли, много се притеснил да не бъде изтеглен кредит на негово име или да не се разпореди някой с имота му; често води разговори на тази тема, като изразявал притесненията си; поведението му се променило, станал мълчалив и угрижен. Съдът намира от правна страна следното:

Както бе посочено, Искът следва да се разгледа по реда на чл. 203 ал.1 от АПК. В случая ответникът по иска-НАП, освен администратор на лични данни, е и адм.орган, поради което по силата на чл. 203 ал.2 от АПК, приложение намира и чл. 1 ал.1 от ЗОДОВ. Искът е предявен срещу ЮЛ /НАП/, в изпълнение на чл. 205 ал.1 от АПК. Ищецът не сочи конкретен орган или дл. лице от НАП, чието незаконосъобразно факт.бездействие е причинило претендираните вреди. Но е посочило точните текстове от ЗЗЛД и Регламента, по които не е било извършено дължимото фактическо действие от администратора на лични данни. От което следва, че твърдяното незаконосъобразно фактическо бездействие е на администратора на лични данни, който се явява адресат на посочените норми от ЗЗЛД и Регламента. За да е предявеният иск основателен, следва съгл. чл. 204 ал.4 от АПК, Съдът да установи дали е налице твърдяното от ищеца незаконосъобразно фактическо бездействие на НАП /или на органи и /или служители на НАП/. Следователно, неоснователно е възражението на ответника, че Искът е неоснователен , тъй като до момента няма влязъл в сила адм. или съд.акт, който да е установил наличието на незаконосъобразно факт. бездействие на НАП. Тъй като Съдът, в рамките на настоящото производство, следва сам да установи дали е налице първата предпоставка за основателност на иска по чл. 1 ал.1 от ЗОДОВ- наличието на незаконосъобразно факт. бездействие. За да е основателен Иска, следва да са налице три кумулативни предпоставки: 1/ установено от Съда незаконосъобразно факт. бездействие на НАП /в качеството на администратор

на лични данни, по посочените от ищеца конкретни текстове на ЗЗЛД и Регламента/; 2/ настъпили вреди/от претендирания вид,размер,естество и период на настъпване/; 3/ причинно-следствена връзка между настъпилите вреди и установеното незаконосъобразно фактическо бездействие, т.е. вредите да са пряка и непосредствена последица от първата предпоставка.

Между страните няма спор, че: **1/ НАП е администратор на лични данни по см. на чл. 4 § 7 от Регламента** / „администратор" означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка/; **2/ че изтеклите данни относно ищеца са лични данни по см. на чл. 4 § 1 от Регламента** /1) „лични данни" означава 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/; **3/ че администраторът НАП обработва личните данни на ищеца по см. на чл. 4 § 2 от Регламента** / „обработване" 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/; **4/ че е налице по см. на чл. 4 § 12 от Регламента „нарушение на сигурността на лични данни"** / 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/.

По първата предпоставка- Съдът установи незаконосъобразно фактическо бездействие на НАП /в качеството на администратор на лични данни/, по чл. 24 и чл. 32 от Регламента и по чл. 45 ал.1 т.6, чл. 59 ал.1, чл. 64 и чл. 66 ал.1 и ал.2 от ЗЗЛД, довело до нарушение на сигурността на личните данни по см. на § 1 т.10 от ДР на ЗЗЛД вр. чл. 4 т.12 от Регламент 2016/679, като **ангажираните от ответника доказателства/при наличие на изрични указания на Съда по доказателствата/, не доказват, че НАП е изпълнил задълженията си на администратор по цитираните норми.** Следва да се има предвид, че ищецът претендира както недостатъчно предприети дължими мерки от администратора по защита на личните данни, така и приложени от администратора недостатъчно ефективни мерки, т.е. **твърди се едновременно липса на достатъчно мерки и наличието на приложени неефективни мерки**.

Съгл. **чл. 24 /“ Отговорност на администратора“/ от Регламента** „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“ . Мерките по чл. 24 § 1 от Регламента включват прилагането на политики, но не се изчерпват само с тях. Няма данни и не се твърди от ответника, че въведените от него мерки по чл. 24 § 1 от Регламента са били периодично преразглеждани и при необходимост актуализирани.Няма данни и не се твърди от ответника да са били одобрени кодекси за поведение по чл. 40 и механизми за сертифициране по чл. 42 от Регламента. Съдът намира поради което, че **администраторът в случая не е в състояние да докаже, че е въвел подходящи техн. и организационни мерки, гарантиращи, че обработва личните данни в съответствие с Регламента.**

Съгл. **чл. 32 /“Сигурност на обработването“/ от Регламента“**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“.

Няма данни и не се твърди от ответника: 1/ да е въвел „псевдонимизация" по см. на чл. 4 § 5 от Регламента /означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че

личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано/; да провежда **редовно изпитване, преценяване и оценка на ефективността** на техническите и организационните мерки с оглед да се гарантира сигурността на обработването; 3/ способност за **гарантиране на постоянна поверителност на системите и услугите** за обработване. Съдът намира поради което, че **администраторът в случая не е в състояние да докаже, че е осигурил сигурността на обработването на данните по см. на чл. 32 от Регламента.**

Съгл. чл. 45 ал.1 т.6 от ЗЗЛД /ред. към 15.07.19г/ „ При обработването на лични данни за целите по чл. 42, ал. 1 личните данни трябва да 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.**

Съдът намира, че **НАП не е общовалидният случай на администратор** на лични данни, **а дър.орган, на когото е поверено създаването, обработването и опазването на данъчната и осигурителната информация относно задължените субекти/**защитена по закон информация с регламентиран достъп до нея/. От което следва, че **изискванията към този администратор, предвид характера и обема на съхраняваната от него информация** /реално това е дан. и осигурителна информация на всички данъчно задължени субекти в РБ, вкл. чужди граждани и чужди ЮЛ/, следва да са чувствително завишени спрямо администратор , обработващ лични данни, които обаче не представляват едновременно и защитена по закон информация. Съдът намира поради което, че **администраторът в случая не е в състояние да докаже, че е гарантира подходящо ниво на сигурност, като е приложил подходящи технически или организационни мерки.**

Съгл. чл. чл. 59 ал.1 от ЗЗЛД /ред. към 15.07.19г/ „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.**Когато това е пропорционално на дейностите по обработване, мерките по ал. 1 включват прилагане от администратора на подходящи политики за защита на данните. Чрез мерки по ал. 1 администраторът **осигурява защита на личните данни на етапа на проектирането**, като отчита достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването на лични данни, както и рисковете за правата и свободите на физическите лица при обработването. **Мерките трябва да са съобразени с изискванията на чл. 45**, **планират се към момента на определяне на средствата за обработването** на лични данни и се **прилагат при самото обработване**. Мерките може да включват **псевдонимизация, свеждане на данните до минимум и въвеждане на необходими гаранции** в процеса на обработване на лични данни. Чрез мерки по ал. 1 администраторът гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, срока на съхраняването им и тяхната достъпност. **Чрез тези мерки се гарантира**, че по подразбиране **без намеса от страна на физическото**

лице личните данни не са достъпни за неограничен брой физически лица“. В случая данните на ищеца са станали достъпни за неограничен брой ФЛ, от което следва, че приложените мерки не гарантират изпълнение на задължението по чл. 59 ал.4 от ЗЗЛД, т.е. **приложените мерки са явно неефективни и не са осигурили защитата на личните данни в достатъчната и необходима степен**. Следователно, **твърдението на ищеца, че мерките са недостатъчно и са неефективни, не се оборва от ответника/носител на доказ.тежест/.**

Съгласно чл. 64 от ЗЗЛД /ред. към 15.07.19г/ „ 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. 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“. Както бе посочено по-горе, **администраторът не е в състояние да докаже, че предприетите от него мерки гарантират в необходимата и достатъчна степен защитата на личните данни.**

Относно чл. 66 ал.1 и ал.2 от ЗЗЛД/ред. към 15.07.19г/ „ 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. **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 ни чрез оборудване за предаване на данни; **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; **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 неоправомощени 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“ . Както сочи самият ответник, **и до момента не е установено кога точно и по какъв начин е станал пробива в инф. система на НАП,** което води до извод на Съда, че НАП не е приложил подходящи технически и организационни мерки за осигуряване , **съобразено с този риск ниво на сигурност автоматизирано обработване** на данни от инф.масиви на НАП.**Не е била гарантирана надеждността на системата /** няма данни за доклади за появили се дефекти във функциите на внедрената система за автоматична обработка на данните/, като **контролът върху носителите на данни, върху съхранението, върху потребителите и върху достъпа до данните** не е бил гарантиран в достатъчната и необходима степен , като прилаганите мерки явно не са били достатъчно ефективни и подходящи.

Съдът намира, че **не е налице твърдяното от ищеца незаконосъобразно фактическо бездействие по чл. 67 от ЗЗЛД.** Съгл. чл. 67 от ЗЗЛД /ред. към 15.07.19г/ „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. 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. 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.Когато не е възможно информацията да се подаде едновременно, тя може да се подаде поетапно без по-нататъшно ненужно забавяне.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.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“. Установява се от

доказателствата по делото, че **на 16.07.19г НАП уведомява КЗЛД за случая, а на 17.07.19г НАП уведомява СГП за случая. На 17.07.19г започва пълен одит на инф.системи на НАП от независима външна организация** с участието на ИТ екипа на приходната администрация.

Съдът намира, че **не е налице твърдяното от ищеца незаконосъобразно фактическо бездействие по чл. 68 от ЗЗЛД.** Съгл. чл. 68 от ЗЗЛД /ред. към 15.07.19г/ „ **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**. 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. 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. 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. 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“.Установено е от данните по делото, че **предвид огромния брой субекти с изтекли лични данни, НАП не е правила индивидуални уведомления до тях**, но чрез медиите на 15.07.19г всички са уведомени за станалия пробив. **НАП е разработил приложение и ел.услуга, чрез които всеки по ЕГН да може да провери** дали и негови лични данни са изтекли, като **конкретно ищецът - на 03.11.19г**, чрез справка в приложението на НАП , **е научил, че и негови лични данни са изтекли.**

Следователно, **по първата предпоставка** за основателност на иска- Съдът установи незаконосъобразно фактическо бездействие на администратора НАП по **чл. 24 и чл. 32 от Регламента и по чл. 45 ал.1 т.6, чл. 59 ал.1, чл. 64 и чл. 66 ал.1 и ал.2 от ЗЗЛД**.

По втората предпоставка- настъпили неимуществени вреди в размер на 1000лв. , Съдът е **указал на ищеца, че носи доказ.тежест относно тяхното настъпване**. От свидетелските показания, които Съдът кредитира /въпреки връзката между свидетеля и ищеца, тъй като **само член на най-близкия кръг на ищеца би имал детайлни наблюдения върху психическото и емоционалното му състояние/,** се установява, че научавайки на 03.08.19г, че са изтекли и негови лични данни/**без да знае какви точно-това научава едва в хода на съд.производство**/, ищецът е започнал да изпитва силно притеснение. То е **продължило във времето и се е задълбочило,** предвид страха на ищеца - дори след изтриване на данните му,те вече са станали

публично достояние и някой може по всяко време да продаде имотите му или да не изтегли кредит на негово име. Съдът намира тези притеснения на ищеца за напълно оправдани и реалистични, а твърдението на ответника за липсата до момента на случай на злоупотреба с изтекли нечий лични данни при пробива , освен недоказано, е и неоснователно. Дори за момента да няма такъв регистриран случай на злоупотреба с изтеклите при пробива лични данни на милиони български граждани /на практика всички данъчно-задължени субекти -ФЛ в РБ/, това не означава, че притеснението е неоснователно и хипотетично. Не са малко известните случаи в РБ за незаконно разпореждане с имоти на гражданите /"имотната мафия" е много активна особено в столицата, където живее и ищецът/, или случаите на теглене на кредити на чуждо име- и без да е имало такъв масиран теч на лични данни. Не е изяснено и до момента - дали изтеклите лични данни не са все още налични на определени места в мрежата /макар и по-трудно достъпни за обикновения потребител на интернет/ , както и дали не са изтъргувани и възможни за злоупотреба в необозримо бъдеще.Съдът намира, че и към момента, и за в бъдеще, ще съществува напълно реален и обоснован риск от злоупотреба с изтеклите данни.Поради което притесненията на ищеца в тази връзка са напълно обосновани. Дори и без свидетелски показания относно конкретното изражение на претендираните неимуществени вреди, Съдът намира, че **самият факт на изтекли публично в интернет лични данни на ищеца, респ. станали потенциално обект на неконтролирана /по време,място и обем/ злоупотреба с тях, обуславят настъпването на неимуществени вреди за субекта на данните**. Следователно, **настъпването на неимуществените вреди следва да се презумира**.

Съдът намира поради което за **доказано** настъпването на неимуществени вреди/**втората предпоставка**/, като те са в **пряка и непосредствена причинно-следствена връзка** с установеното по-горе незаконосъобразно фактическо бездействие на администратора. **Доказана е и третата предпоставка** за основателност на иска.

Относно размера на вредите: Вредите са настъпили **след 03.11.19г** /когато ищецът е разбрал, че и негови данни са изтекли в нета/, като се търпят от ищеца и към момента. Доколкото **администраторът е ЮЛ, то отговорността му е обективна** и не е необходимо изследване на виновно поведение у конкретен служител на НАП. Размерът на тези неимуществени вреди следва да се определи **по справедливост от Съда** /съгл. чл. 52 от ЗЗД/, но не само предвид характера и степента на преживените вътрешни душевни страдания и чувство на страх и тревожност, но и **предвид обема на изтеклите данни /само ЕГН/.** В конкретния случай, Съдът намира по справедливост, че една пета от претендираните 1000 лв, а именно- 200лв, са **справедливо обезщетение за негативните преживявания на ищеца, които преживявания за съжаление обосновано ще продължат и занапред** и няма основание да се счита, че вече са неоснователни.

Относно претендираните лихви- доколкото Съдът уважава главния иск за вреди, то следва да се уважи и акцесорния иск за лихви. Претендират се лихви , считано от увредата на 15.07.19г, или алтернативно- от датата на ИМ. Съдът намира, че **увредата не е настъпила на 15.07.19г, а на неустановена все още дата/когато е станал пробива**/. На 15.07.19г само е станало публично известно, че са увредени неопределен кръг лица. На 03.11.19г /при справката в приложението на НАП/, ищецът е научил, че е сред увредените лица, но това не променя факта, че е увреден по-рано/преди 15.07.19г/. Съдът намира обаче, че лихвата следва да се присъди от

датата на предявяване на иска за вреди – 16.09.19г /в този смисъл и практиката на ВАС, след известни колебания/, тъй като преди тази дата ищецът не е претендирал обезщетение, а респ. ответникът не е дължал такова/не му е поискано все още/.
Относно разноските: Съгл. чл. 10 ал.3 от ЗДОИ, Ако искът бъде уважен изцяло или частично, съдът осъжда ответника да заплати разноските по производството, както и да заплати на ищеца внесената държавна такса. Съдът осъжда ответника да заплати на ищеца и възнаграждение за един адвокат или юрисконсулт, ако е имал такъв, **съразмерно с уважената част от иска**. Ищецът е заплатил 10лв дър.такса по делото, 30лв. за частна жалба пред ВАС , няма други разноски, като е защитаван от адвокат на осн. 38 ал.2 вр. ал.1 т.3 от ЗА.Съдът на осн. чл. 38 ал.2 от ЗА следва да определи адвокатско възнаграждение в размер не по-нисък от този по чл. 8 ал.1 т.1 от Наредба № 1/04г /който е 300лв/, но съгл. чл. 10 ал.3 от ЗОДОВ- съобразно уважената част от иска. Следователно, при материален интерес по делото-1000лв, мин.размер адв.хонорар за уважен изцяло иск е 300лв. В такъв случай, **при една пета уважен иск,** мин.размер би следвало да е 60 лв. **На осн. чл. 38 ал.2 от ЗА**, Съдът следва да присъди **на адв. Ю. адв.хонорар** не по-малко от **60лв/съобразно уважената част от иска/. На ищеца- 40лв** за платени по делото/вкл. пред ВАС/- **дър.такси.**
Съгл. чл. 10 ал.4 от ЗОДОВ, Съдът осъжда ищеца да заплати на ответника възнаграждение за един адвокат, ако е имал такъв, **съразмерно с отхвърлената част** от иска, а в полза на юридическите лица се присъжда възнаграждение, ако те са били защитавани от юрисконсулт, чийто размер **не може да надхвърля максималния размер за съответния вид дело, определен по реда на чл. 37 от Закона за правната помощ.** Съгл. чл. 25 ал.1 от Наредбата за заплащане на правната помощ вр. чл. 37 ал.1 от ЗПП, мин.юрисконсултско възнаграждение при дело с мат.интерес е 100лв. При юрисконсултско възнаграждение за изцяло отхвърлен иск- 100лв, **на ответника** следва да се присъди **80 лв юрисконсултско възнаграждение съобразно отхвърлените четири пети части от иска.**
Водим от горното и на осн. чл. 39 ал.2 от ЗЗЛД, чл. 203 и сл. от АПК вр. чл. 1 ал.1 от ЗОДОВ, Съдът

РЕШИ:

ОСЪЖДА Национална агенция по приходите да заплати на Е. А. Г. от [населено място] сумата от **200лв /двеста лева/**, представлява обезщетение за причинените му неимуществени вреди, ведно със **законната лихва, считано от 16.09.19г** до окончателното изплащане на сумата, по Искова молба вх.№ 27810/16.09.19г на Е. А. Г. от [населено място], с която е предявен Иск по чл. 39 ал.2 от ЗЗЛД 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/ против администратор на лични данни - НАП, с цена на иска 1000лв, представляващи обезщетение за причинените неимуществени вреди от незаконосъобразно фактическо бездействие на НАП да изпълни задълженията си по чл. 24 и чл. 32 от Регламента и по чл. 45 ал.1 т.6, чл. 59 ал.1, чл. 64, чл. 66 ал.1 и ал.2, чл. 67 и чл. 68 от ЗЗЛД, довело до нарушение на сигурността на личните данни по см. на § 1 т.10 от ДР на ЗЗЛД вр. чл. 4 т.12 от Регламент 2016/679 и допуснат пробив в информационната система на НАП с резултат- публично разгласяване на личните данни на около 5 000 000 български граждани /граждани на ЕС/, станало публично известно чрез медиите на 15.07.19г.

ОСЪЖДА Национална агенция по приходите да заплати на Е. А. Г. от [населено място] сумата от **40 лв/четиридесет лева**/, представляваща разноски по делото **и по д.№ 2646/20г на ВАС.**

ОСЪЖДА Национална агенция по приходите да заплати на адвокат С. Ц. С.-Ю. сумата от **60лв /шестдесет лева**/, представляваща адвокатско възнаграждение по чл. 38 ал.2 от ЗА, **съобразно уважената една пета част от иска.**

ОТХВЪРЛЯ предявения иск в останалата му част- над 200лв до предявения размер от 1000лв.

ОСЪЖДА Е. А. Г. от [населено място] да заплати на Национална агенция по приходите сумата от **80 лв/осемдесет лева**/, представляваща разноски по делото, **съобразно отхвърлените четири пети части от иска.**

РЕШЕНИЕТО подлежи на обжалване с касационна жалба пред ВАС в 14дневен сок от съобщението.

Съдия: