Р Е Ш Е Н И Е
№ 13833

гр. София, 05.08.2024 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 50 състав,** в публично заседание на 04.06.2024 г. в следния състав:

СЪДИЯ: Мария Бойкинова

при участието на секретаря Ива Лещарова, като разгледа дело номер **919** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145, ал. 2, т. 1 и сл. от Административно-процесуалния кодекс (АПК).

Образувано е по жалба на „Ай енд Джи Иншурънс Брокерс“ ЕООД, чрез процесуалния представител адв. И. Г., срещу решение № ПАИКД-13-33/2023 г. от 08.01.2024 г. на Комисията за защита на личните данни, с което на основание чл. 58, § 2, буква „г“ от Регламент (ЕС) 2016/679 за нарушение на § 1, буква „е“ във връзка с чл. 32, § 1, буква „б“ и чл. 5, § 2 във връзка с чл. 24, § 1 и § 2 от Регламент (ЕС) 2016/679 се издава разпореждане на дружеството в качеството на администратор на лични данни да извърши анализ риска, въз основа който да определи подходящи технически и организационни мерки за защита на личните данни и да приеме вътрешен писмен документ(политика/правила/процедура), който да регламентира обработването на лични данни чрез информационната система WEBBROKER и на основание чл. 58, § 2, буква „и“ от Регламент (ЕС) 2016/679 е наложено административно наказание - имуществена санкция в размер на 50 000 лева.

С жалбата се твърди, че при постановяване на оспореното решение са допуснати съществени нарушения на административнопроизводствените правила, противоречие с материалноправните разпоредби, несъответствие с целта на закона и неспазване на установената форма. С жалбата се излагат доводи, че не е налице нерегламентиран пробив в системите на дружеството, както и че личните данни на засегнатите субекти не са били засегнати от външно лице. Наред с това се оспорва извода на административния орган, че субектите на лични данни, които са засегнати от

инцидента са 40 000, както и че нарушението е извършено през VPN акаунт на разработчика. Поддържа се, че вътрешните документи по отношение на системата Webbroker са в съответствие с изискванията на закона, както и че дружеството има вътрешни правила и процедури по отношение на техническите характеристики и защита на личните данни. Твърди се в жалбата, че дружеството стриктно изпълнява изискванията на ОРЗД за отчетност на действията по обработка на личните данни, разделяне на данните по потоци, категории, субекти, проследяване на тяхното предоставяне на лица и организации извън „Ай енд Джи Иншурънс Брокерс“ ЕООД. Твърди се също така, че дружеството е направило детайлна оценка на риска, тъй като функционалността на системата е организирана по начин, по който данните за клиенти, данните за полици и за плащане по полиците са записани в различни структури и не се съдържа информация за ЕГН и ЕИК на клиент, а има само данни за номер на полица, вид застраховка, клиент и телефон. Оспорва се констатацията в решението, че липсва информация какви данни се обработват през Webbroker и какъв е срокът за съхранение на данните, като се посочва, че в почти всички документи, които дружеството е представило в КЗЛД са описани данните, които се обработват през Webbroker, а именно: имена и ЕГН за служителите и имена, ЕГН, адрес, телефонен номер, имейл и номер за МПС. Според жалбоподателя действията на дружеството както по време на инцидента, така и след това са в съответствие с изискванията на ОРЗД, поради което на дружеството не може да се вмени вина за инцидента, още по-малко да му се налага наказание. Твърди се, че незаконосъобразно е определен размера на наложената имуществена санкция в противоречие с чл. 83, § 4 и 5 ОРЗД. Искането до съда е да се отмени изцяло оспореното решение като незаконосъобразно, както и да се присъдят сторените по делото разноски..

Ответникът - Комисията за защита на личните данни се представлява юрк. К., която оспорва жалбата, като излага съображения за законосъобразност на оспореното решение, като поставено при спазване на материалния закон и административнопроизводствените правила.

Административен съд – София град, като взе предвид изложените от страните доводи и събраните по делото доказателства, намира следното от фактическа страна :

Не се спори между страните, а и от представените и приети писмени доказателства се установява, че на 19 и 20.08.2023 г. жалбоподателят е получил три писма по електронната поща от злонамерени трети лица, като в две от тях са били приложени три снимки от меню „Картотеки“ на информационната система, с която същият борави, и с твърдения, че тези лица притежават общо 15GB данни, файлове и справки на жалбоподателя.

Поради съдържанието на писмата и евентуалното съмнение за пробив в информационната система, оспорващото дружество съгласно задълженията му по Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (ОРЗД) и в срока по чл. 33, ал .1 от същия е подал уведомление до КЗЛД за нарушение сигурността на личните данни по чл. 33 от ОРЗД с вх. № ПАИКД-13-33/22.08.2023 г. Наред с това дружеството е организирало вътрешна проверка по случая с участието на М. М. - ръководител на информационни и комуникационни технологии при жалбоподателя, И. Д., отговарящ за развитието и поддръжката на информационната система на жалбоподателя, експерти от Р., отговарящи за предоставянето на сървърната инфраструктура, както и С. Д. – външен системен администратор. Проверката е материализирана в доклад с дата 22.08.2023 г., според който няма външен пробив в

информационната система на дружеството, няма никакви изтеглени данни от сървъра съхраняващ същите, тъй като достъпът до същия е невъзможен през публично достъпна интернет връзка, а само чрез административен достъп до него. Също така вътрешните експерти правят предположение, че изтичането на посочените снимкови данни в злонамерените имейли е възможно да е от компрометирана работна станция, с оглед на това, че с правата на достъп, които имат повечето потребители, няма как да бъде достъпена базата данни през работна станция. Докладът след това описва какви мерки са предприети след получаване на заплашителните имейли и завършва с изброяване на планираните бъдещи мерки с цел повишаване на сигурността.
Докладът от 22.08.2023 г. както и допълнителната информация изискана от КЗЛД, в т.ч. документация относно мерките и процедурите предприети от оспорващото дружеството преди и след 19-ти и 20.08.2023 г. са представени на административния орган.
След извършен анализ на риска от страна на КЗЛД, с решение на 20.09.2023 г. е възложено извършване на проверка по документи на дружеството.
Последвали са още искания за предоставяне на допълнителни документи и информация от страна на КЗЛД към жалбоподателя, които същият предоставя, вкл. и допълнителен доклад с дата 06.10.2023 г. изготвен от М. М. и И. Д., в който подробно се анализират направените снимки от меню „Картотеки“, като същите стигат до заключението, че снимките са направени от трето лице с достъп до системата от вида „супер-потребител“, който не притежава нужните права за достъп до сървъра съдържащ базата данни, за разлика от администраторския акаунт, който притежава повече такива. Според доклада единственият, който може да установи връзка със сървъра съдържащ базата данни, която в злонамерените имейли се твърди да е компрометирана, е И. Д., включително и чрез неговия point to point VPN акаунт, но според представената информация, няма данни подобен достъп да е бил осъществен от него. Също така е посочено, че ако И. Д. е осъществил съответния достъп и е направил снимки от неговата работна станция, то според докладите, както и според вещото лице от допуснатата по делото СКЕ, тези екранни снимки ще изглеждат по различен начин или с друг „интерфейс“. В доклада от 06.10.2023 г. се съдържа и извадка на потребители, които са влизали в информационната система между 09.01.2023 г. и 31.07.2023 г., като отново се посочва, че няма нерегламентиран достъп до сървъра с базата данни, която в злонамерените имейли от 19 и 20.08.2023 г. се твърди да е компрометирана.
Видно е от представеното по делото писмо вх. № ПАИКД-13-33# 10/18.2023 г., че жалбоподателят е предоставил на КЗЛД попълнен „Въпросник за извършване на проверки при осъществяване на надзорната дейност на КЗЛД“, заедно с приложени към него документи, вкл. „Описание на правата на достъп на служителите/администраторите до системата с приложение към него в табличен вид – права за достъп за всички служители“, „Атестационна карта относно съответните корпоративни стандарти и изисквания на ОРЗД“, „Описание на техническите характеристики и мерки за защита на личните данни при ползване на _информационната система“, Анализ на риска за правата и свободите на физическите лица, във връзка с обработването на техните данни във връзка с получената заплаха на 19.08.2023 г., протоколи от обучението относно практическо прилагане на ОРЗД на служителите на „Ай енд Джи Иншурънс Брокерс“ ЕООД през 2018 г., копия на подписани присъствени списъци от служителите, преминали обучение по защита на

личните данни, протокол за проведено продължаващо обучение през 2019 г., 2020 г., 2021 г. и 2022 г. с копия на подписани присъствени списъци на служителите, преминали обучение по защита на личните данни и Инструктаж за приложимите при дружеството жалбоподател вътрешни правила за мерките за защита на личните данни, съгласно Регламент 2016/679.
Установява се, че с писмо с изх. № ПАИКД-13-33#11/30.10.2023 г. КЗЛД е изискала от жалбоподателя още допълнителна информация във връзка с изясняване обстоятелствата около инцидента, която е била предоставена с писмо с вх. № ПАИКД-13-33#12/02.11.2023 г.
С писмо с изх. № ПАИКД-13-33#15/09.11.2023 г. от жалбоподателя е била изискана и допълнителна информация относно броя на клиентите, чиито лични данни дружеството обработва, чрез информационната система към момента на нарушението на сигурността на личните данни, която също е била предоставена.
На 08.01.2024 г. КЗЛД се произнася с решение № ПАИДК-13-33/2023 г., в което констатира нарушения на сигурността на личните данни от страна на оспорващото дружество и определя административно наказание – имуществена санкция на стойност 50 000 лв. в изпълнение на целите на чл. 83, § 4, б. „а“ за нарушение на чл. 24, § 1 и § 2, чл. 25, § 1, чл. 28, § 1, чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/679 и чл. 8, § 5, буква „а“ за нарушение на чл. 5, § 1, б. „е“ и § 2 от Регламент (ЕС) 2016/679.
По делото служебно е допуснато изслушването на съдебно-компютърна експертиза за изясняване на спорните между страните факти и обстоятелства, имащи релевантно отношение към предмета на спора. При извършен от вещото лице анализ на операционно-информационната система на жалбоподателя от горепосочените доклади в резултат от двете вътрешните проверки на същия, се потвърждава от него, че снимките посочени в злонамерените имейли на 19 и 20.08.2023 г. са направени от работната станция на лице с достъп до системата на ниво „супер-потребител“. Също така вещото лице потвърждава, че лице с правомощия на „супер-потребител“ не може да сваля лични данни съхранявани в сървъра на системата. Вещото лице разяснява, че снимките са направени от отдел „Картотеки“ в системата на жалбоподателя, който позволява задаване на заявки от съответните потребители на базата на определени данни, които конкретния потребител притежава. Според експерта на ниво „супер-потребител“ не е възможно лицето да се сдобие с лични данни на трети лица, ако преди това не притежава лични данни за същите лица, които в отдел „Картотеки“ са ограничени до три имена и адрес. Вещото лице потвърждава, че външен достъп до сървъра е невъзможен и следователно няма пробив в системата на жалбоподателя. В допълнение, вещото лице твърди, че функционалността на системата на жалбоподателя е организирана така, че данните за клиенти, данните за полици, за плащане се записват в различни структури с цел сигурност, нещо, което се твърди от жалбоподателя както в кореспонденцията си с КЗЛД, така и в жалбата си до Административен съд – София град. В заключение според вещото лице, въведените технически и организационни мерки в системата на жалбоподателя отговарят на настоящите изисквания на пазара от гледна точка на информационната сигурност, а използването на „Облачна“ среда, гарантира на друго ниво надеждността, съхранението на данните и достъпването на системата.
При така установената фактическа обстановка съдът приема следното от правна страна :
В процесния случай, като основание за ангажиране на

административно-наказателната отговорност на жалбоподателя чрез налагане на имуществена санкция в размер на 50 000 лева, административният орган конкретизира твърдяното бездействие от страна на служители на „Ай енд Джи Иншурънс Брокерс“ ЕООД, като неполагане на достатъчна грижа и не прилагане на ефективни мерки за защитата на сигурността на данните, с което не са изпълнени задължения, произтичащи от чл. 24, § 1 и § 2, чл. 25, § 1, чл. 28, § 1, чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/679 и чл. 8, § 5, буква „а“ за нарушение на чл. 5, § 1, б. „е“ и § 2 от Регламент (ЕС) 2016/679.

Съгласно чл. 59, ал. 1 от ЗЗЛД 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. Същото задължение се съдържа и в чл. 24 от Общия регламент относно защита на личните данни (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г., а в чл. 32 от регламента са предвидени конкретните мерки които следва да се предприемат.

Също така и съгласно чл. 66, ал. 1 ЗЗЛД 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 ЗЗЛД, като съгласно чл. 66, ал. 2 (т. 1-т. 11) ЗЗЛД по отношение на автоматизираното обработване администраторът или обработващият лични данни след оценка на рисковете прилагат мерки, имащи за цел да се осъществява контрол върху достъпа до оборудване - като се откаже достъп на неоправомощени лица до оборудването, използвано за обработване на лични данни (т. 1), контрол върху носителите на данни - да се предотврати четенето, копирането, изменянето или отстраняването на носители на данни от неоправомощени лица (т. 2); 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; както и контрол върху пренасянето (т. 3) и да се осъществи 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 (т. 8).

Не е спорно между страните, а и се установи от обсъдените по-горе писмени доказателства, че на 19-ти и 20 август 2023 г. дружеството „Ай енд Джи Иншурънс Брокерс“ЕООД е получило заплашителни имейли с искане за заплащане на суми в биткойни, за да се избегне продажбата на достъпени „общо 15 GB данни, файлове и справки“. Получени са общо три имейла, „подписани от екипът на Crimecorp“ изпратени от recet [електронна поща] и [електронна поща] с твърдения, че разполагат с „десетки хиляди уникални полици от няколко клона на I&G, изкарани чрез Scarpe от панелите“. Към електронните съобщения са приложени екранни снимки от меню картотеки на информационната система на дружеството.

С оглед на това безспорно се установява по делото, че е налице противоправно

деяние, което обаче съдът намира, че само по себе си не обосновава извод, че е следствие от незаконосъобразното бездействие на дружеството жалбоподател да изпълни произтичащи от посочените по-горе разпоредби на регламента и закона задължения да осигури достатъчна надеждност и сигурност на информационната си система и да се защитят физическите и юридически лица, клиенти на дружеството, във връзка с обработването на личните им данни и че не е резултат от престъпно деяние по смисъла на Наказателния кодекс, както и който резултат да е настъпил въпреки положените усилия за предотвратяването му. В процесния случай безспорно е налице противоправно поведение от страна на трети лица, довело до негативния резултат - неоторизиран достъп до базата данни на дружеството жалбоподател, съдържащи информация за имена, ЕГН, адрес и телефонен номер и имейл на служители и клиенти на дружеството. Обратно на възприетата от административния орган теза, този негативен резултат не презюмира противоправно поведение на администратора на лични данни, изразяващо се в бездействие на последния да приложи подходящи технически и организационни мерки за осигуряване защитата на базата данни така, че срещу нея по никакъв начин, от никого и с никакви средства да не може да бъде достъпено. Възприемането на тази теза би означавало, че всеки, който е станал обект на каквото и да било неправомерно посегателство, следва да понесе отговорност, че е допуснал извършването на същото, тъй като не е положил достатъчно грижи за предотвратяването му. В тази връзка за доказване изпълнение на задълженията си, произтичащи от регламента и закона, жалбоподателят е представил по делото множество писмени доказателства, като изготвени и приети: „Описание на правата на достъп на служителите/администраторите до системата, с приложение към него в табличен вид – права за достъп за всички служители“, „Атестационна карта относно съответните корпоративни стандарти и изисквания на ОРЗД“, „Описание на техническите характеристики и мерки за защита на личните данни при ползване на информационната система“, Анализ на риска за правата и свободите на физическите лица, във връзка с обработването на техните данни във връзка с получената заплаха на 19.08.2023 г., протоколи от обучението относно практическо прилагане на ОРЗД на служителите на дружеството през 2018 г., копия на подписани присъствени списъци от служителите, преминали обучение по защита на личните данни, протокол за проведено продължаващо обучение през 2019 г., 2020 г., 2021 г. и 2022 г. с копия на подписани присъствени списъци на служителите, преминали обучение по защита на личните данни и Инструктаж за приложимите при дружеството жалбоподател вътрешни правила за мерките за защита на личните данни, съгласно Регламент ЕС) 2016/679.

Посочените документи са приети като доказателства по делото и не са оспорени от ответника. Както се установява от заключението на приетата и неоспорена от страните СКЕ, при извършения от вещото лице технически анализ на изработената от жалбоподателя операционна система и правилата за

разпределение на функционалностите в нея измежду служителите на дружества, че функционалността на изработената от дружеството система за защита на операционната система е организирана така, че данните за клиенти, данните за полици, за плащане и др. се записват в различни структури с цел сигурност, както и че са въведени редица технически и организационни мерки, които отговарят на актуалното състояние на техниката от гледна точка на информационната сигурност, като в тях е заложено използването на „облачна среда“, която да гарантира на друго ниво надеждността, съхранението на данните и достъпването на системата. По отношение на технологията за сигурност в операционната система са заложени два вида проследяване: на ниво операционна система и на ниво Webbrocker, като в последния случай е изградена единна „лог“ система, от която да може да се проследява последователността и точното време на действията на всеки потребител от момента на влизане в системата до момента на излизане, както на определени оператори, така и на цели процеси. Системата също така позволява и анализ на трафика, който да покаже дали е в обичайните му стойности и дали има някакво завишаване или занижаване, както такъв е направен и при анализа на инцидента, като е установено своевременно наличието на значителен трафик определен период преди инцидента, както и че същият няма връзка с настъпването му.

От заключението на вещото лице се установява и обстоятелството, че на базата на направения анализ и на информацията видима в изведените справки от системата, може да се направи най-вероятният извод, че снимките получени от злонамереното трето лице са направени най-вероятно от работната станция на потребител с права и роля на „супер- потребител“ съобразно информационната система Webbrocker, като заснемането им е станало в момент при който работната станция е била в режим на работа „офлайн“.

Същевременно функционалността на информационната система Webbrocker не позволява и не дава информация за структурата, таблиците в базата данни през установения потребител с роля „супер-потребител“, като лице с такива права разполага с достъп само до конкретно избрани данни, групирани по дефинирани правила и при наличие на допълнителна информация/данни за въвеждане, като базата данни, която се съхранява на отделен сървър може да бъде изтеглена само с административен достъп до сървъра, а това изключва възможността базата данни да бъде изтеглена от лице с потребителски достъп. Лице с потребителски достъп, от чиято работна станция се установява, че са заснети личните данни, не разполага с възможност да изтегли цялата база данни съдържащи се в сървъра, нито да се изтеглят такива количества файлове, за които се твърди в писмото от злонамереното лице. Базата данни може да бъде изтеглена само от лица с административен достъп, но както се установява от заключението на вещото лице достъпът на лицата с административен достъп (в т.ч. и на разработчикът на системата) е от съвсем друг интерфейс и злонамерените снимки не са направени от негов достъп. Това от своя страна

опровергава извода, следващ се от констатациите в Констативния акт за извършената проверка на „Ай енд Джи Иншурънс Брокерс“ ЕООД с рег.№ ПАИИД-13-33413/06.11.2023 г., резултатите от който са послужили като фактическо основание за издаване на оспореното решение, че течът на личните данни от операционната система на жалбоподателя е вследствие на евентуални злонамерени действия на разработчика на програмата, респ. на друго лице от организационната структура на дружеството, разполагащо с пълен достъп на административни права до всички функционалности на системата (с роля на MasterCode по смисъла на утвърдените от дружеството описание на правата на достъп на служителите- администраторите на данни до системата Webbrocker). Както се установи по безспорен начин от експертизата достъпването само до ограничена част от съхраняваните лични данни на клиентите и служителите на „Ай енд Джи Иншурънс Брокерс“ ЕООД е станало посредством работна станция на лице, ползващо ограничените права на „супер-потребител“ и то в състояние на режим „офлайн“ на станцията чрез заснемането на екрана на монитора на вече запаметени данни, което от своя страна с оглед ограничения характер на заснетите лични данни, изключва предполагаем извод за недобронамерена намеса от страна на което и да е лице с административни права, даващи му възможност до пълен достъп до информацията съдържаща се в сървъра. Извод в тази насока е и безспорно установената от вещото лице констатация, че не са налице данни за изтичане на лични данни в посочения в заплашителните писма значими размери.

При така установеното по делото съдът намира, че не е налице твърдяното от административния орган незаконосъобразно бездействие на жалбоподателя, намиращо израз в неприлагане на подходящи технически и организационни мерки, вкл. и на етап проектиране на информационно-операционната система WEBBBROKER, целящи предотвратяване настъпването на нарушението. Изтичането на част от данните от операционната система на жалбоподателя е вследствие на недобросъвестни и злонамерени действия от страна на трети лица, при които с оглед липсата на доказателства действително да са изтекли данните в посочените от тези лица размери, както и това, че създадената и приложената от жалбоподателя операционна система съответства и напълно отговаря на съвременните технологични изисквания за запазване и съхраняване на информацията, вкл. и от злонамерени действия на трети лица, изключва извод, че са налице основанията за ангажиране на административно-наказателната отговорност на жалбоподателя като администратор на лични данни, на основание чл. 83, § 4, б. „а“ за нарушение на чл. 24, § 1 и § 2, чл. 25, § 1, чл. 28, § 1, чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/679 и чл. 8, § 5, буква „а“ за нарушение на чл. 5, § 1, б. „е“ и § 2 от Регламент (ЕС) 2016/679.

По така изложените съображения оспореното от жалбоподателя „Ай енд Джи Иншурънс Брокерс“ ЕООД решение № ПАИКД-13-33/2023 г. от 08.01.2024 г. на Комисията за защита на личните данни следва да бъде отменено като

незаконосъобразно.
На основание чл. 143, ал. 3 АПК ответникът Комисия за защита на личните данни следва да бъде осъден да заплати на жалбоподателя направените от него съдебно-деловодни разноски по производството в общ размер на 11 411,49 лева.

По изложените съображения съдът,

Р Е Ш И :

ОТМЕНЯ решение № ПАИКД-13-33/2023 г. от 08.01.2024 г. на Комисията за защита на личните данни, с което на основание чл. 58, § 2, буква „г“ от Регламент (ЕС) 2016/679 за нарушение на § 1, буква „е“ във връзка с чл. 32, § 1, буква „б“ и чл. 5, § 2 във връзка с чл. 24, § 1 и § 2 от Регламент (ЕС) 2016/679 се издава разпореждане на дружеството в качеството на администратор на лични данни да извърши анализ риска, въз основа който да определи подходящи технически и организационни мерки за защита на личните данни и да приеме вътрешен писмен документ(политика/правила/процедура), който да регламентира обработването на лични данни чрез информационната система WEBBROKER и на основание чл. 58, § 2, буква „и“ от Регламент (ЕС) 2016/679 е наложено административно наказание - имуществена санкция в размер на 50 000 лева.
ОСЪЖДА Комисията за защита на личните данни да заплати на „Ай енд Джи Иншурънс Брокерс“ ЕООД, ЕИК[ЕИК], сумата в размер на 11 411,49 лева, представляваща разноски по производството.
Решението подлежи на обжалване пред Върховния административен съд в 14-дневен срок от съобщаването му.

СЪДИЯ: