Р Е Ш Е Н И Е
№ 29511

гр. София, 23.07.2026 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 50 състав,** в публично заседание на 09.06.2026 г. в следния състав:

СЪДИЯ: Мария Бойкинова

при участието на секретаря Ива Лещарова, като разгледа дело номер **10789** по описа за **2025** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145 и следващите Административно-процесуалния кодекс (АПК).

Образувано е по жалба на „Специализирана очна болница за активно лечение Акад. Пашев“ ЕООД, ЕИК[ЕИК], представлявано от управителя Д. П. М., чрез адв. М., срещу Решение № ПАИКД-13-16/2024 г. от 15.09.2025 г. на Комисията за защита на личните данни (КЗЛД, Комисията), с което на основание чл. 58, § 2, буква „г“ от Регламент (ЕС) 2016/679 за нарушение на чл. 5, § 1, буква „е“ във връзка с чл. 32, § 1, буква „б“ и буква „г“ и чл. 5, § 2 от Регламент (ЕС) 2016/679 на дружеството жалбоподател, в качеството му на администратор на лични данни, е издадено разпореждане да регламентира извършването на периодичен анализ на риска и да предвиди във вътрешните си документи спазване на принципите на отчетност и извършване на периодичен одит, и на основание чл. 58, § 2, буква „и“ от Регламент (ЕС) 2016/679 му е наложена имуществена санкция в размер на 70 000 (седемдесет хиляди) лева, съгласно чл. 83, § 5, буква „а“ от Регламента, за същото нарушение.

С жалбата се твърди, че оспореното решение е незаконосъобразно като постановено при съществени нарушения на административнопроизводствените правила, в противоречие с материалния закон и в несъответствие с целта на закона. Според жалбоподателя КЗЛД не е извършила дължимия анализ, като направи преценка на естеството, тежестта и продължителността на нарушението, вземе предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда. Според жалбоподателя КЗЛД не е взела предвид техническите и организационните мерки, въведени от лечебното заведени в съответствие с чл. 25 и 32 Регламент

(ЕС) 2016/679. Твърди се, че КЗЛД не е приложила Методиката за определяне нивото на риска при нарушения на сигурността на личните данни, както и че в решението не е разяснено как е приложена Методика за определяне нивото на риска при нарушения сигурността на личните данни, за да се стигне до извода в решението, че рискът е бил висок.
Твърди се в жалбата, че не са налице каквито е да доказателства, от които да се следва, че е налице загуба на поверителността, тъй като при извършена проверка след инцидента е било установено, че няма данни за изтегляне или копиране на данните, обект на атаката.
Оспорват се като неверни констатациите в решението, че в резултат на атаката е можело да се стигне до невъзможност от отчитане на предоставените от жалбоподателя услуги пред НЗОК за периода на нарушението. Изтъква се, че лечебното заведение е отчело пред НЗОК извършените в периода от 08.02.2024 г. до 16.02.2024 г. дейности, когато са били предоставени услуги на здравноосигурени пациенти.
На следващо място се твърди, че оспореното решение не е съответно на целта на закона - съгласно чл. 1. ал. 2 във връзка с чл. 2, ал. 2 от ЗЗЛД, а именно: да гарантира неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите и юридическите лица при неправомерно обработване на свързаните с тях лични данни, доколкото не са налице доказателства каква част от засегнатите лични данни са били копирайки/изтеглени от страна на третото лице.
Излагат се съображения, че неправилно КЗЛД е определила размера на имуществената санкция съгласно чл. 83, § 5, буква „а“ за нарушение на чл. 5, § 1, буква „е“ вр. чл. 32, § 1, буква „б“ и буква „г“ и чл. 5, § 2 от Регламента, като жалбоподателят счита същата за прекомерна и не отговаряща на установеното нарушение, предвид неговите конкретни специфики и последици.
Жалбоподателят поддържа, че предприетите от него технически и организационни мерки са съответствали на актуалните към момента на инцидента изисквания за информационна сигурност.
Иска се отмяна на решението изцяло, евентуално - намаляване на наложената санкция, както и присъждане на направените по делото разноски. В представени по делото писмени бележки подробно се излагат съображения за основателността на жалбата.
Ответникът - Комисията за защита на личните данни, чрез процесуалния си представител, оспорва жалбата като неоснователна и моли решението да бъде потвърдено, като поддържа, че въведените от администратора мерки не са били достатъчни да предотвратят инцидента, а размерът на наложената санкция е определен в съответствие с критериите по чл. 83, § 2 от Регламента. В представени по делото писмени бележки подробно се излагат съображения за законосъобразността на оспореното решение.
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 приетите по делото писмени доказателства се установява, че на 08.02.2024 г. в 03:00 ч. срещу компютърната система на „Специализирана очна болница за активно лечение Акад. Пашев“ ЕООД е осъществена кибератака, изразяваща се в нерегламентиран достъп от IP адрес 2.57.149.200.
Не се спори между страните, че в законоустановения 72-часов срок дружеството е подало до КЗЛД уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679 с вх. № ПАИКД-13-16/14.02.2024 г..
По повод на уведомлението от служители на КЗЛД е извършена проверка на място и по документи, при която са снети екранни разпечатки от автоматизирани информационни системи на СОБАЛ „Акад. Пашев“ ЕООД. За резултатите от проверката е съставен Констативен протокол,

съгласно който в резултат на извършената през нощта на 07.02 срещу 08.02.2024 г. злонамерена атака към компютърната мрежа на лечебното заведение системните файлове на операционните системи на сървърите и програмните продукти (Гама Кодмастър, Гама Стоп. Гама Конт) за регистрация на пациентите и управление на медицинската дейност в лечебното заведение, както и базите данни и архивните файлове на тези програми, са били „заразени“ със злонамерен софтуер от вида „Ransomware“. Проверяващите са установили, че от лог файловете на входящия рутер е изолиран източника на кибератаката - неоторизиран достъп от IP 2.57.149.200, с евентуално местонахождение в Руската федерация, [населено място], интернет доставчик LIR Limited, Datacenter. Констатирано е при проверката, че след „заразяването“ тези файлове са криптирани и на практика неизползваеми и недостъпни, както и че локалните работни станции в кабинетите на лекарите и административния персонал на болницата не са засегнати от атаката. Проверяващите са установили, че в мрежата на лечебното заведение е разпространен BackMyData рансъмуер вирус от групата на Phobos Ransomware - злонамерен софтуер, който криптира файлове на системите и заплашва с унищожаването им, ако не бъде платена поисканата сума. Установили са, че в инфраструктурата на СОБАЛ „А.. П.“ се съдържа информация, че мрежата е компрометирана и файловете са криптирани, като атакуващите не само криптират данните, но и твърдят, че са ги откраднали, заплашвайки да ги публикуват, ако откупът не бъде платен, като се представят като „бизнесмени“, които не искат да навредят, а само да получат пари. Предоставят имейл за контакт: [електронна поща]“ - Това потвърждава, че е вирусът вариант на Phobos рансъмуер, известен като „Backmydata“ - едно от многото разширения, които рансъмуер вирус Phobos добавя към криптирани файлове.

Въз основа на констатациите от проверката КЗЛД е обосновала извод, че е налице нарушение на наличността на данните и най-вероятно на поверителността, изразяващо се в достъп, преднамерена загуба и унищожаване на обработваните от администратора СОБАЛ „А.. П.“ лични данни на физически лица. В решението са изложени съображения, че има вероятност данните да са все още налични, тъй като администраторът е загубил контрол или достъп до тях или същите са унищожени и поради факта, че не съществуват във вид, в който може да бъдат използвани, което представлява загуба на наличността на данните. Обоснован е извод, че с атаката сериозно са засегнати правата и интересите на засегнатите субекти, тъй като това е могло да доведе до отлагане предоставяне на медицинска услуга, поради необходимост от запознаване с резултати от предходни прегледи и изследвания, както и поради невъзможност от отчитане предоставяне на услугите пред НЗОК за периода на нарушението. Посочено е в решението, че са засегнати данни на 15 779 физически лица (32 122 записа), от които 106 лица под 18-годишна възраст, включително данни за физическа идентичност, социална идентичност и специални категории данни по чл. 9 от Регламента, свързани със здравния статус на пациенти.

По горните съображения КЗЛД е приела, че нарушението е с „високо ниво на риск“, и с Решение № ПАИКД-13-16/2024 г. от 15.09.2025 г. е издала разпореждане по чл. 58, § 2, буква „г“ и е наложила имуществена санкция от 70 000 лева по чл. 58, § 2, буква „и“ от Регламента, приемайки, че администраторът не е приложил подходящи технически и организационни мерки по смисъла на чл. 24 и чл. 32 от Регламент (ЕС) 2016/679.

По делото е допусната и приета съдебно -компютърна експертиза (СКЕ), изготвена от вещото лице д-р инж. Н. Н. Х.. От заключението на вещото лице, което съдът кредитира изцяло като компетентно, обективно и обосновано, се установява следното: компютърната мрежа на жалбоподателя е защитена чрез рутер с конфигуриран firewall, като мрежата е от затворен тип без отворени портове към външния свят, а достъпът до нея се осъществява единствено чрез VPN връзка с определен списък от оправомощени IP адреси. Вещото лице е посочило, че физически

сървърите се намират в специално оборудвано сървърно помещение, което отговаря на приложимите изисквания.

При изходящ капацитет на връзката от 1 Gbps и установен времеви прозорец на потенциален неовладян достъп от около 1 час (от 05:19 ч. до 06:13 ч.), теоретично максимално възможният обем за ексфилтрация е около 200–225 GB, а при реалистични мрежови условия - между 135 и 180 GB, поради което вещото лице заключава, че ексфилтрация на обем от порядъка на 10 TB в рамките на посочения времеви прозорец е технически невъзможна. Според заключението всички модули на Интегрирана информационна система „Гама консулт" са били засегнати от злонамерената атака, като е извършено преинсталиране, което е приключило на 14.02.2024 г. и от тази дата е било възможно повторно въвеждане на базата данни, изискуемата информация в информационната система и преустановяване ръчно изготвяне на документите за текущите услуги. Вещото лице посочва, че не са били засегнати локалните станции в лекарските кабинети и администрацията.

Съгласно заключението единствено незасегнат е бил един архив във файловия сървър, който е бил копиран на отделен външен носител и сканиран с антивирусни програми, за да се установи безопасността му за евентуално използване. Наложило се е форматиране на твърдите дискове и на трите сървъра, като драстично решение за справяне с инфекцията от зловредната програма, като всички сървърни конфигурации са били преинсталирани и цялата компютърна мрежа е изградена отново.

Според заключението, въведените технически и организационни мерки - както към момента преди инцидента, така и мерките, предприети след него са адекватни на изискванията за информационна сигурност.

При така установената фактическа обстановка съдът приема следното от правна страна:

Съгласно чл. 59, ал. 1 ЗЗЛД и чл. 24 от Регламент (ЕС) 2016/679, 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 приложимото право. Конкретните мерки, които следва да се предприемат, са уредени в чл. 32 от Регламента, съответно в чл. 66 ЗЗЛД.

Съгласно постановеното от Съда на Европейския съюз по дело C-340/21 (Решение от 14.12.2023 г.), членове 24 и 32 от Регламент (ЕС) 2016/679 следва да се тълкуват в смисъл, че неразрешеното разкриване на лични данни или неразрешеният достъп до тях от трето лице по смисъла на чл. 4, точка 10 от Регламента сами по себе си не са достатъчни, за да се приеме, че приложените от администратора технически и организационни мерки не са „подходящи“ по смисъла на посочените разпоредби. Преценката дали приложените мерки са подходящи следва да се извърши от националните юрисдикции конкретно, като се вземат предвид рисковете, свързани със съответното обработване, и се прецени дали естеството, обхватът и прилагането на тези мерки са съобразени с тези рискове. В същия смисъл е и практиката на Върховния административен съд като например Решение № 8668 от 07.10.2022 г. по адм. д. № 3441/2022 г., V отделение, съгласно което възприемането на тезата, че при осъществен неправомерен достъп до данни винаги е налице нарушение на чл. 32, § 1 от Регламента, без значение от предприетите преди нарушението мерки, би довело до обективна отговорност на всеки администратор, станал жертва на посегателство от трети лица - резултат, който противоречи на смисъла и целите на закона. Именно за да се избегне подобен извод, административният орган дължи конкретно изследване и преценка на съществувалите преди нарушението мерки за защита на данните и на това дали те са били подходящи и съобразени с достиженията на техническия прогрес, разходите за прилагане,

естеството, обхвата, контекста и целите на обработването, както и с рисковете с различна вероятност и тежест за правата и свободите на физическите лица.
В настоящия случай не се спори, а и от доказателствата по делото се установява по несъмнен начин, че на 08.02.2024 г. дружеството жалбоподател е станало обект на противоправно поведение от страна на трети лица - масова ransomware атака, довела до неоторизиран достъп до информационната му система. Този негативен резултат сам по себе си обаче не презюмира незаконосъобразно бездействие на администратора по смисъла на чл. 24 и чл. 32 от Регламента. Обратното би означавало всеки администратор, станал обект на каквото и да е неправомерно посегателство, автоматично да носи административнонаказателна отговорност, независимо от предприетите от него мерки за сигурност — извод, изрично отхвърлен както от практиката на СЕС и на ВАС, така и от практиката на настоящия съд.
От кредитираното от съда заключение на съдебната компютърно-техническа експертиза се установява по безспорен начин, че към момента на инцидента компютърната система на лечебното заведение е включвала три сървъра - два HYPER-V инсталирани сървъри и един файлов сървър, който се използва за съхранение на копия на данните от другите два сървъра. Системата е конфигурирана, като HYPER-V CLUSTER, като освен на файловия сървър, бекъп на информацията се прави и на всеки от основните сървъри, като архивите се съхраняват на отделна виртуална машина за резерв. Компютърната мрежата е защитена с рутер с конфигуриран Firewall, като мрежата е от затворен тип т.е. няма отворени портове за външния свят, а влизането е само чрез VPN достъп с определен списък IP адреси, имащи право на достъп.
Установява се също така, че реакцията на служителите на жалбоподателя след получаване на автоматичната аларма в 03:17 ч. е била своевременна и адекватна, довела до прекъсване на интернет свързаността в 06:13 ч. - действие, което съобразно неоспореното заключение на вещото лице е осуетило възможността за ексфилтрация на данни в твърдения от нападателите обем, доколкото такава ексфилтрация в рамките на наличния времеви прозорец и мрежов капацитет е била технически невъзможна. Това означава, че макар файловете на болницата да са били криптирани, не е установено със сигурност, че данните са напуснали системата и съответно са били достигнали до трети лица. В подкрепа на това е и обстоятелството, че не са налице данни за подавани жалби и сигнали от пациенти или служители на лечебното заведение. Според съда въпросът за евентуална ексфилтрация на лични данни е спорен, доколкото вещото лице след като е извършило технически анализ на мрежовия капацитет и времевия прозорец, в рамките на който е съществувала техническа възможност за изходящ трансфер на данни, заключава, че ексфилтрацията на обем от 10 TB е технически невъзможна. Този си извод вещото лице обосновава с факта, че при изходящ капацитет от 1 Gbps и активен прозорец от приблизително 54 минути (05:19 ч. – 06:13 ч. на 08.02.2024 г.), максималният теоретично възможен обем за ексфилтрация е около 200–225 GB, а при реалистична мрежова ефективност - 135-180 GB. Следователно твърдението от страна на нападателите, че са откраднали 10 TB данни е технически опровергано от вещото лице и не може да послужи като основание за предполагаема ексфилтрация в посочения обем, каквото е твърдението на КЗЛД. От горното следва извода, че отговорността на администратора на лични данни следва да се преценява при отчитане на тази неопределеност, като доказателствената тежест за установяване на конкретната ексфилтрация лежи върху КЗЛД.
Съдът приема, че по делото не е доказано по несъмнен начин да е осъществен трансфер на лични данни към трети неоправомощени лица вследствие на кибератаката. При тези обстоятелства не може да се приеме за установено настъпването на неразрешено разкриване на лични данни по смисъла на чл. 4, т. 12

от GDPR. Не се споделя извода на КЗЛД, че администраторът на лични данни в пълна степен носи отговорност за настъпването на нарушението на сигурността на личните данни, тъй като не е бил е предприел подходящи технически и организационни мерки за защита поверителността и наличността на личните данни, преди констатирания инцидент-хакерска атака. Установява се по делото, че информационната система на лечебното заведение използва система за сигнализиране на необичайни действия – IDS, която в 03:17 ч. на 08.02.2024 г. е изпратила имейл до системните администратори. В резултат на това, реалната работа на хакерите по криптиране на данните е започнала в 05:19 ч., тъй като до този момент се е работило по създаването на потребители с подходящи права, като в 6.10 часа е прекъсната на интернет връзката в сградата. Така за около 1 час служителите са успели да осуетят ексфилтрация на данни видно от заключението на вещото лице. Действително злонамерената атака е причинила тотално унищожаване на операционните системи и конфигурациите на всички три сървъра, но от друга страна следва да се вземе и предвид факта, че своевременно е била преизградена цялата мрежова инфраструктура, включително чрез преинсталиране на болничния софтуер - Интегрирана информационна система „Гама консулт" - и инициализация на базите данни, като процесът на възстановяване е приключил на 14.02.2024 г. Установено е, че мрежовата инфраструктура на лечебното заведение е разполагала с технически защитни мерки - конфигуриран хардуерен защитен екран (firewall), мрежа от затворен тип без отворени портове към интернет, достъп единствено чрез VPN с ограничен списък от разрешени IP адреси, и физическа сигурност на сървърното помещение. Тези мерки според съда са в съответствие с изискването на чл. 32 от GDPR за прилагане на подходящи технически и организационни мерки за защита на личните данни. В тази връзка съдът намира за неоснователно възражението на ответника, че от експертизата не се установявало информационната система на лечебното заведение да е използвала система за сигнализиране на необичайни действия - IDS. Твърденията на ответника, че снимките от съобщенията до администратора са компрометирани е защитна теза, която не се подкрепя от доказателствата по делото. Именно защото системата е сигнализирала за неоторизиран достъп администраторът на лични данни веднага е започнал работа по изясняване на ситуацията.

Фактът, че въпреки наличните защити е реализирана успешна атака чрез компрометиране на VPN достъп, не означава автоматично, че мерките са били недостатъчни, доколкото релевантен критерий е дали те са съответствали на нивото на риска към момента на инцидента, а не дали са се оказали абсолютно непробиваеми. Предприетите от болничното заведение мерки преди инцидента са достатъчни за постигане на основните цели на мрежовата и информационна структура, доколкото според вещото лице изградената защита чрез рутер с конфигуриран firewall, мрежа от затворен тип без отворени портове към външния

свят, с достъп до нея единствено чрез VPN връзка с определен списък от оправомощени IP адреси, представлява адекватна конфигурация, отговаряща на изискванията за безопасност към 2024 г. В подкрепа на горното е извода на вещото лице, че достъпът е осъществен по легитимен технически канал (VPN) - вероятно чрез компрометирани идентификационни данни, а не чрез пробив в защитните системи като такива. Това разграничение е съществено, тъй като насочва отговорността към въпроса за управлението на идентификационните данни и процедурите за достъп, а не към архитектурата на мрежата.

Наред с това следва да се отбележи, че в периода от атаката до пълното възстановяване на системите не е било спирано обслужването на пациентите в болничното заведение, тъй като е имало архив на хартиен носител, нито пък това е препятствало отчитането на клиничните пътеки пред НЗОК, каквото е твърдението на КЗЛД. Следва да се отбележи също така, че локалните работни станции в лекарските кабинети и администрацията не са били засегнати. Реализирането на атаката при тези обстоятелства следва да се квалифицира като външно събитие с висока степен на сложност, а не като резултат от неизпълнение на нормативно установени задължения от страна на администратора, който своевременно е осуетил и ограничил възможността за ексфилтрация.

При така установените факти съдът приема, че по делото не е доказано по несъмнен начин да е осъществен трансфер на лични данни към трети неоправомощени лица вследствие на кибератаката. Съгласно чл. 32 от GDPR администраторът на лични данни е длъжен да приложи подходящи технически и организационни мерки, като се вземат предвид съвременното развитие на технологиите, разходите за изпълнение, естеството и контекстът на обработването и рисковете за правата на физическите лица, тоест не се изисква абсолютна непробиваемост, а съразмерност с реалния риск.

В този смисъл предприетите от жалбоподателя технически и организационни мерки за защита на личните данни мерки отговарят на установените добри практики в областта на информационната сигурност и надхвърлят минималните изисквания, приложими за организации от съответния мащаб. Видно от заключението на вещото лице, което се е позовало на международно утвърдения онлайн портал за киберсигурност и ИТ новини - BleepingComputer. BleepmgComputer, е че след анализ на над 100 случая с подобен тип пробив, към момента няма публично потвърдени индикации или независими данни, че при ransomware атаката срещу болнични информационни системи в Румъния и България през февруари 2024 г. е настъпило реално изтичане на чувствителни пациентски или лични данни, въпреки заявките на нападателите за кражба на такива.

Безспорно се установява по делото, че в съответствие с изискванията на чл. 24, § 2 от Регламент (ЕС) 2016/679, от лечебното заведение са утвърдени вътрешни документи, свързани със защитата на личните данни, както следва: Правилник за

защита на личните данни в на „Специализирана очна болница за активно лечение Акад. Пашев“ ЕООД, Инструкции относно механизма на обработване на лични данни, Вътрешни правила за мрежова и информационна сигурност, Методика за извършване на оценка на риска, Процедура за действия при нарушения на сигурността на личните данни и за уведомяване за нарушение, Уведомление до контрагентите за обработването на лични данни при договори с лечебното заведение, Уведомление за обработването на лични данни във връзка с трудови правоотношения, Уведомление за защита на лични данни и конфиденциалност, предоставяни във връзка с предоставяне на медицински услуги. Горните документи са анализирани от КЗЛД, която изрично в решението е посочила, че същите определят основните принципи на обработване на лични данни, целите, основанията и начините на обработване; сроковете за съхранение на лични данни, начините за упражняване на правата от субектите на данни, техническите и организационни мерки за защита на данните, действията при нарушение на сигурността на личните данни, вътрешната организация и отчетност на дружеството.

Неоснователно е възражението на ответника, че атаката е в резултат на недоброто обучение на служителите, тъй като е било възможно вирусът да е бил задействан чрез линк на отворен от служител имейл. Действително според вещото лице това е възможен вариант, но тъй като по делото няма категорични доказателства, че в случая достъпът до информационната система е станал точно по този начин, не следва да се обсъжда тази възможност.

По изложените съображения изводът на КЗЛД, че администраторът не е приложил подходящи технически и организационни мерки, не намира опора в доказателствата по делото, а обжалваното решение не съдържа конкретен анализ кои точно мерки административният орган приема за неподходящи и по какви съображения, съпоставени със заключението на вещото лице.

При липса на установено по надлежния ред неизпълнение на задълженията по чл. 24 и чл. 32 от Регламент (ЕС) 2016/679, не са налице материалноправните предпоставки за издаване на разпореждане по чл. 58, § 2, буква „г“ от Регламента, нито за ангажиране на административнонаказателната отговорност на жалбоподателя и налагане на имуществена санкция на основание чл. 58, § 2, буква „и“ във връзка с чл. 83, § 5, буква „а“ от Регламента. Поради това обжалваното решение се явява постановено в противоречие с материалния закон и следва да бъде отменено изцяло като незаконосъобразно.

При този изход на спора и на основание чл. 143, ал. 1 АПК, на жалбоподателя се дължат направените по делото разноски, съгласно представения списък по чл. 80 ГПК, включващи заплатена държавна такса, възнаграждение за допуснатата и приета съдебн0-компютърноекспертиза и адвокатско възнаграждение, общо в размер на 3116.95 евро.

По изложените съображения съдът,
Р Е Ш И :
ОТМЕНЯ Решение № ПАИКД-13-16/2024 г. от 15.09.2025 г. на Комисията за защита на личните данни, с което на „Специализирана очна болница за активно лечение Акад. Пашев“ ЕООД, ЕИК[ЕИК], на основание чл. 58, § 2, буква „г“ от Регламент (ЕС) 2016/679 за нарушение на чл. 5, § 1, буква „е“ във връзка с чл. 32, § 1, буква „б“ и буква „г“ и чл. 5, § 2 от Регламент (ЕС) 2016/679 е издадено разпореждане да регламентира извършването на периодичен анализ на риска и да предвиди във вътрешните си документи спазване на принципите на отчетност и извършване на периодичен одит, и на основание чл. 58, § 2, буква „и“ от Регламент (ЕС) 2016/679, съгласно чл. 83, § 5, буква „а“, е наложена имуществена санкция в размер на 70 000 (седемдесет хиляди) лева.
ОСЪЖДА Комисията за защита на личните данни да заплати на „Специализирана очна болница за активно лечение Акад. Пашев“ ЕООД, ЕИК[ЕИК], сумата в размер на 3116.95 евро, представляваща направени по делото разноски.
Решението подлежи на обжалване пред Върховния административен съд в 14-дневен срок от съобщаването му на страните.

СЪДИЯ: