Р Е Ш Е Н И Е
№ 10788

гр. София, 30.04.2026 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 15 състав,** в публично заседание на 21.04.2026 г. в следния състав:

СЪДИЯ: Росица Цветкова

при участието на секретаря Антонина Митева, като разгледа дело номер **10788** по описа за **2025** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145 и сл. от АПК във връзка със Закона за защита на личните данни и Регламент (ЕС) 2016/679.

Делото е образувано по жалба на „Специализирана очна болница за активно лечение „Вижън“ ЕООД със седалище и адрес на управление: [населено място], [улица], чрез Адвокатско дружество „Г., Т. и КО“ срещу Решение № ПАИКД-13-15/2024 г. от 15.09.2025 г. на Комисията за защита на личните данни, с което на дружеството, в качеството му на администратор на лични данни, са дадени разпореждания за привеждане на операциите по обработване на лични данни в съответствие с изискванията на Регламент (ЕС) 2016/679 и му е наложена имуществена санкция в размер на 100 000 лева за нарушение на чл. 5, § 1, б. „е“ във връзка с чл. 32, § 1, б. „б“ и б. „г“ и чл. 5, § 2 от Регламент (ЕС) 2016/679. Жалбоподателят твърди, че решението е незаконосъобразно, постановено при неправилно установена фактическа обстановка, при неправилно приложение на материалния закон и в нарушение на принципа на съразмерност. Поддържа се, че не е доказано настъпило нарушение на поверителността на личните данни, нито изтичане или разпространение на данни извън информационната система на дружеството. Излага

се, че лечебното заведение е било обект на външна кибератака, за която своевременно са уведомени компетентните органи, включително КЗЛД, като са предприети действия за ограничаване на последиците и възстановяване на работата на системите. Иска се отмяна на решението. Претендират се разноски.

Ответникът – Комисията за защита на личните данни, оспорва жалбата и поддържа законосъобразността на издадения акт. Счита, че в хода на административното производство са установени пропуски в техническите и организационните мерки за защита на личните данни, включително относно архивирането, периодичната оценка на риска и одита на информационните системи, които обосновават наложените коригиращи мерки и имуществената санкция. Претендира се присъждане на юрисконсултско възнаграждение.

Съдът, след като обсъди доводите на страните и събраните по делото доказателства, приема за установено от фактическа страна следното:

Административното производство пред КЗЛД е образувано след уведомление от СОБАЛ „Вижън“ ЕООД за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679. В уведомлението е посочено, че на 08.02.2024 г. в 03:00 часа лечебното заведение е станало обект на хакерска атака, в резултат на която е изгубен достъпът до използваните специализирани софтуери, съдържащи лични данни на пациенти и служители, като сървърите са били криптирани и недостъпни, а от извършителите е поискано заплащане на парична сума за възстановяване на достъпа до данните. В хода на производството КЗЛД е изискала допълнителна информация, извършена е проверка, съставени са докладна записка, констативен протокол и констативен акт.

В хода на административното производство от КЗЛД до СОБАЛ „Вижън“ ЕООД е изпратено Писмо с изх. № ПАИКД-13-15#1/21.02.2024 г., с което е изискана допълнителна информация за изясняване на фактите и обстоятелствата във връзка с получения сигнал /л.36-37/. Постъпил е отговор от СОБАЛ „Вижън“ ЕООД с вх. № ПАИКД-13-15#2/26.02.2024 г., с който е предоставена информация и документи по запитването на КЗЛД /л.38-78/.

Впоследствие от КЗЛД до СОБАЛ „Вижън“ ЕООД е изпратено Писмо с изх. № ПАИКД-13-15#3/05.03.2024 г., с което болничното заведение е уведомено, че от представения от него отговор

и документи от 26.02.2024 г. не могат да се изяснят фактите и обстоятелствата, относими към конкретния случай. В тази връзка от СОБАЛ „Вижън“ ЕООД е изискано в 7-дневен срок да представи конкретна информация, описана в писмото на административния орган от т. 1 до т. 6 /л.79/. В указания срок от СОБАЛ „Вижън“ ЕООД с Писмо вх. № ПАИКД-13-15#4/12.03.2024 г., е предоставена информация по поставените с писмото шест въпроса /л.80-82/.

С писмо вх. № ПАИКД-13-15#5/22.03.2024 г., от страна на СОБАЛ „Вижън“ ЕООД е предоставена информация и документи относно лицето Й. Г., заемащ в болничното заведение длъжността Администратор Информационни системи /л.83-89/. След извършен анализ, съобразно Методика за определяне на нивото на риска при нарушения на сигурността на личните данни, е изготвена Докладна записка с рег. № ПАИКД-13-15#6/25.03.2024 г., с която е определено „Високо ниво на риск“. В тази връзка с решение на КЗЛД от 27.03.2024 е възложено извършване на проверка на място на администратора на лични данни.

С Писмо изх. № ПАИКД-13-15#7/24.06.2024 г. на КЗЛД, СОБАЛ „Вижън“ ЕООД е уведомено за извършване на проверка по случая. Към уведомлението за проверка е приложен и Въпросник за проверка /л.90-94/. С Писмо вх. № ПАИКД-13-15#8/22.07.2024 г., от страна на администратора на лични данни е предоставена информацията по поставените въпроси, като е приложен комплект документи под опис от СОБАЛ „Вижън“ ЕООД съгласно дадените указания /л.95-131,л.144-180/.

Със Заповед № РД-15-266/26.06.2024 г., издадена от Председател на КЗЛД е наредено извършване на проверка по спазване и прилагане на Регламент /ЕС/ № 2016/679 и ЗЗЛД на СОБАЛ „Вижън“ ЕООД. С издадената заповед е определен съставът на проверяващия екип, както и задачата на проверката, включително указания до екипа /л.139/. Заповедта е връчена лично и срещу подпис на управителя на проверяваното болнично заведение в качеството му на администратор на лични данни на 05.12.2024 г. /л.139/.

Проверката на място е открита на 05.12.2024 г., разяснени са задачите и начина на нейното протичане, осъществен е оглед на автоматизирани информационни системи, обсъдени са следните въпроси: категориите физически лица, до чиито данни е осъществен неоторизираният достъп; категориите лични данни и видове информация, станали достъпни при неоторизирания достъп; предприети мерки в 72-часовия срок от узнаване за нарушението на сигурността; предприети мерки за уведомяване на засегнатите субекти и за минимализиране на вредите;

постъпили сигнали и жалби за конкретното нарушение на сигурността; документация от извършената вътрешна проверка по казуса; документацията относно одита на информационните системи и електронните услуги преди и след осъществения нерегламентиран достъп; извършената оценка на риска за правата и свободите на физическите лица; предприетите технически и организационни мерки за защита на данните, в т.ч на системите, чрез които е осъществен неоторизираният достъп.

Резултатите от проверката са обективирани в Констативен протокол от 05.12.2024 г., като са снети екранни разпечатки от автоматизираните информационни системи на СОБАЛ „Вижън“ ЕООД, като всички документи и изискана информация са приложени към Преписка с рег. № ПАИКД-13-15/14.02.2024 г. /л.181/. След приключване на проверката от страна на проверяващия екип е съставен Констативен акт с рег. № ПАИКД-13-15#9/24/19.06.2025 г., в който подробно са описани извършените действия и приобщени документи и информация, респективно какво е установено в хода на проверката /л.132-138/.

Обобщените резултати от проверката се изразяват в следното:

1. Действително възникнало събитие в СОБАЛ „Вижън“ ЕООД, представляващо случай на нарушение на сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент /ЕС/ № 2016/679. Установено нарушение на наличността на данните и най-вероятно на поверителността, изразяващо се в достъп, преднамерена загуба и унищожаване на обработваните от администратора СОБАЛ „Вижън“ ЕООД лични данни на физически лица. Загубен контрол върху тези данни от страна на администратора, както и че той вече не ги притежава;

2. В СОБАЛ „Вижън“ ЕООД не е извършен вътрешен/външен одит относно сигурността на информационните системи преди нарушението на сигурността;

3. В СОБАЛ „Вижън“ ЕООД е извършен вътрешен одит относно сигурността на информационните системи след нарушението на сигурността;

4. В СОБАЛ „Вижън“ ЕООД е извършвана оценка на риска относно сигурността на информационните системи преди нарушението на сигурността, която е с дата 15.02.2019 г. Не са представени доказателства, доказващи твърденията на администратора, че оценката на риска

относно сигурността е преразглеждана през 2021 г. и през 2023 г.;

5. В СОБАЛ „Вижън“ ЕООД е извършена оценка на риска след нарушението от дата 09.02.2024 г.;

6. Не са налични сертификати за информационна сигурност и за защита на личните данни;

7. Не са представени доказателства, доказващи твърденията на администратора за периодично извършвани подходящи вътрешни тестове на сигурността на информационната система;

8. От страна на СОБАЛ „Вижън“ ЕООД не са предприети необходимите мерки за създаването на копия /резервни копия за възстановяване/ и архивиране на информацията. Утвърдените процедури и политики за архивиране/бекъпи на информационните системи са общо прилагащи се и не са съобразени спрямо конкретното обработване. Бекъпите и базите данни се съхраняват на същите дискови масиви, както и съответните бази данни. Същите са криптирани при хакерска атака;

9. Администраторът на лични данни е допуснал загуба на способност за предоставяне на критична услуга. Отменени са няколко операции, при които не може в цялост да се възстанови медицинската документация. Въпреки това няма медицински случаи на животозастрашаващи състояния към момента на проверката.

В хода на проверката от страна на администратора е съобщено, че вследствие на инцидента са отменени няколко операции, при които не може в цялост да се възстанови медицинската документация. От негова страна е наведен довод, че не е налице установено нарушение на поверителността и/или целостта на данните, независимо от липсата на доказателства, подкрепящи това твърдение. От проверяващите е установено, че съгласно вътрешните правила на СОБАЛ „Вижън“ ЕООД, по отношение на архивиране/бекъпи на информационните системи са общо прилагащи и не са съобразени спрямо конкретното обработване. СОБАЛ „Вижън“ ЕООД уведомява проверяващите, че не е извършван одит от външно лице или независима вътрешна служба на информационните системи на лечебното заведение преди и след настъпилото събитие. От СОБАЛ „Вижън“ ЕООД е изискана информация и документи относно одит на информационните му системи преди и след нарушението на сигурността. Администраторът на лични данни не е представил информация за извършени вътрешни одити преди инцидента, нито

са представени от него и доказателства за това. В отговор 10, раздел III от Въпросника от администратора е само потвърдено, че не са извършвани външни одити. Вътрешна проверка е извършена след нарушението на сигурността, обективирана в представено с преписката становище на А. Г. – ДЛЗД, експерт в отдел „Информационни технологии“, СОБАЛ „Вижън“ ЕООД. Проверяващият екип е установил, че администраторът на лични данни е извършил оценка на риска след инцидента за правата и свободите на физическите лица при обработване на личните им данни, като от него е направен извод, че съществува вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица. Установено е, че Оценката на риска е от дата 09.02.2024 г., изготвена съгласно утвърдена от дружеството Методика за извършване на оценка на риска. От страна на СОБАЛ „Вижън“ ЕООД е представена последната извършена Оценка на риска преди атаката, която е с дата 15.02.2019 г. Анализът на същата според проверяващите, показва висок риск за правата и свободите на субектите на данни, чиито лични данни са обработвани от администратора. В тази връзка проверяващият екип е стигнал до извод, че е трябвало да се приемат допълнителни технически и организационни мерки, включително регулярно извършване на оценка на риска, чрез която да се разгледат специфичните рискове, произтичащи от обработването на лични данни. Прието е още, че администраторът на лични данни е следвало да въведе стриктни механизми, позволяващи му осъществяване на завишен контрол върху данните, както и да не допуска неоторизиран пробив в сигурността на обработваните данни. Не са представени доказателства, подкрепящи твърденията на администратора за извършена оценка на риска през 2021 г. и 2023 г. От извършената вътрешна проверка, администраторът не установява да е осъществен неоторизиран достъп до лични данни, както и извършван трансфер на данни, поради което от негова страна е счетено, че не установено нарушение на поверителността и/или целостта на данните, за което обаче не са представени безспорни доказателства.

В рамките на проверката е констатирано още, че в СОБАЛ „Вижън“ ЕООД не е внедрен стандарт ISO 27701, информационните системи за обработка на лични данни не са сертифицирани по отношение на сигурността. Отчетено е сътрудничеството на администратора в хода на проверката и предприетите от негова страна допълнителни технически и организационни мерки за справяне с нарушението на сигурността на данните, както и уведомяването на КЗЛД в срок от 72 часа от узнаване за нарушението по реда на чл. 33 от Регламент /ЕС/ № 2016/679. Независимо от това от

проверяващия екип е направен извод, че независимо от действията на администратора, последиците от нарушението са необратими.

Административният орган е приел, че е налице нарушение на сигурността на личните данни, изразяващо се в загуба на наличността на данните и вероятно засягане на тяхната поверителност. Като съществени пропуски са посочени липсата на доказателства за актуална оценка на риска след 2019 г., липсата на извършен одит на информационните системи преди инцидента, липсата на сертификати за информационна сигурност и най-вече недостатъчната организация на архивирането, доколкото резервните копия и базите данни са били съхранявани на същите дискови масиви и са били засегнати от криптирането.

На свое заседание, проведено на 10.07.2025 г., КЗЛД е приела Констативен акт с рег. № ПАИКД-13-15#9/24/19.06.2025 г. и е взела единодушно решение за налагане на административно наказание „имуществена санкция“ и издаване на разпореждане до СОБАЛ „Вижън“ ЕООД, в качеството му на администратор на лични данни да съобрази операциите по обработване на лични данни с разпоредбите на Регламент /ЕС/ № 2016/679.

Въз основа на така проведеното административно производство е издадено оспореното решение, с което на основание чл. 58, § 2, б. „г“ и б. „и“ вр. чл. 83, § 5, б. „а“ за нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ и б. „г“ вр. чл. 5, § 2 от Регламент /ЕС/ № 2016/679:

/т. 1/ на администратора на лични данни е разпоредено: да регламентира извършването на периодичен анализ на риска, въз основа, на който да определи подходящи технически и организационни мерки за защита на личните данни; да предвиди в своите вътрешни документи спазване на принципите на отчетност и извършване на периодичен одит с цел проверка на съответствието спрямо изискванията на Регламент /ЕС/ № 2016/679; да бъдат утвърдени/ актуализирани процедури и политики за архивиране/бекъпи на информационните системи, което да позволи надеждно и своевременно възстановяване; да предостави изготвена и утвърдена документация по отношение на одобрени ръководства за защита на информационните системи, които по време на проверката са посочени в процес на изготвяне от СОБАЛ „Вижън“ ЕООД. Указан е срок на изпълнение на даденото разпореждане – три месеца от датата на влизането на решението на КЗЛД;

/т. 2/ на администратора на лични данни наложено административно наказание - имуществена санкция в размер на 51 129.19 евро или 100 000.00 лева за нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ и б. „г“ вр. чл. 5, § 2 от Регламент /ЕС/ № 2016/679, като размерът на наказанието е определен на основание чл. 83, § 5, б. „а“.

Във връзка със спорните по делото обстоятелства, допуснато ли е нарушение от жалбоподателя, в какво се изразява то, по делото е изслушано заключението на вещото лице по компютърно-техническа експертиза. Според заключението атаката е осъществена чрез ransomware, вариант от семейството Phobos/BackMyData, като е налице ръчно управлявана атака, при която нападателят е получил отдалечен достъп до системата и е стартирал криптиране на файловете. Вещото лице е приело, че от лог файловете е изолиран източникът на атаката, че системата е сигнализирала за необичайни действия и че след установяване на инцидента служителите са предприели действия за прекъсване на достъпа до интернет, с което е осуетен евентуален трансфер на данни. Заключението съдържа и извод, че ексфилтрация на обем от приблизително 10 TB данни в рамките на около един час е технически невъзможна. Същевременно вещото лице е пояснило в съдебно заседание, че не е разполагало с възможност да изследва самите машини, че липсват достатъчно запазени логове и че част от изводите са направени въз основа на предоставени от жалбоподателя снимки на екран на сървърите към момента на атаката. Обективни данни за мерките преди това са взети на база логовете до 02.02.2024г. Заключението е подробно и обосновано, поради което съдът го кредитира в частта относно вида на атаката, предприетите действия за реакция, липсата на установени данни за ексфилтрация и техническата преценка относно невъзможността за трансфер на посочения обем данни в установения времеви интервал, като същевременно съобразява направените от вещото лице уточнения относно липсата на достъп до първичните машини и непълнотата на запазените логове.

Представените по делото заповеди № № 6 и 9 от 2021г. и № 4 и № 5 от 2023г. на управителя на лечебното заведение за възлагане извършване оценка на риска и оценка на въздействието на обработването на лични данни, респективно за потвърждаване на оценките от 2019г., представляват частни диспозитивни документи и не се ползват с достоверност относно датата на съставянето им. Доколкото същите не са били представени в хода на административната проверка, а едва в съдебното производство, съдът приема, че първата достоверна дата на тези заповеди е датата на представянето им по делото, а именно през февруари 2026г. Не са налице

доказателства, установяващи по несъмнен начин извършване на актуална оценка на риска през 2021 г. и 2023 г.

Решението на КЗЛД е било съобщено на жалбоподателя и жалбата до съда е подадена в рамките на предвидения от закона срок за обжалването му.

При така установеното от фактическа страна съдът намира жалбата за процесуално допустима, като подадена в срок, от адресат на оспорения акт, който има правен интерес от съдебното му оспорване.

Разгледана по същество, жалбата е частично основателна.

Оспореното решение е издадено от компетентен орган, в предвидената от закона форма и при спазване на административнопроизводствените правила. Комисията е действала в рамките на правомощията си като национален надзорен орган по Регламент (ЕС) 2016/679. Обстоятелството, че производството е започнало по уведомление на самия администратор по чл. 33 от Регламента, не ограничава правомощията на КЗЛД да извърши проверка и при установено нарушение да приложи коригиращите мерки по чл. 58, § 2 от Регламента, както и да наложи административно наказание при условията на чл. 83 от същия регламент. Уведомяването за нарушение на сигурността не е самоцелно действие, а механизъм, чрез който надзорният орган се сезира за настъпило събитие, за да прецени както естеството на нарушението, така и адекватността на въведените от администратора технически и организационни мерки. Административното производство е проведено по реда на чл. 63 от Правилника, който урежда действията на КЗЛД при подадено уведомление по чл. 33 от ОРЗД. Противно на релевираните в жалбата доводи, административният орган детайлно е разяснил и обсъдил приложението на Методика за определяне на риска при нарушения на личните данни. Неоснователно е възражението, че имуществената санкция е следвало да бъде наложена по общия ред на ЗАНН чрез съставяне на АУАН и издаване на наказателно постановление. Производството е проведено по специалния ред, предвиден за действията на КЗЛД при подадено уведомление по чл. 33 от Регламент (ЕС) 2016/679. След приключване на проверката комисията разполага с правомощията по чл. 58, § 2 от Регламента, включително да приложи коригиращи мерки и да наложи административна имуществена санкция по чл. 83 от Регламента. Поради това общият ред по ЗАНН не намира

приложение като условие за валидност на санкционното произнасяне.

При преценка на съответствието на решението с материалния закон, съдът съобрази следното: Съдът не споделя възраженията на жалбоподателя, че в случая изобщо не е налице нарушение на сигурността на личните данни. Съгласно чл. 4, т. 12 от Регламент (ЕС) 2016/679 „нарушение на сигурността на личните данни“ е нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване на или достъп до лични данни, които се предават, съхраняват или обработват по друг начин. Нормата обхваща не само случаите на доказано разкриване или изтичане на данни, но и случаите на загуба, унищожаване или компрометиране на наличността им. В случая безспорно е установено, че вследствие на кибератаката информационните системи на лечебното заведение са били блокирани, сървърите са били криптирани, а достъпът до обработваните в тях лични данни е бил временно невъзможен. Това обуславя наличие на нарушение на сигурността най-малкото в аспекта на наличността на данните.

Съдът приема също, че правилно КЗЛД е преценила, че администраторът не е доказал въвеждането на достатъчно подходящи технически и организационни мерки по смисъла на чл. 32 от Регламент (ЕС) 2016/679. Съгласно тази разпоредба администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки, за да осигурят съобразено с риска ниво на сигурност, включително способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент, както и процес на редовно изпитване, преценяване и оценяване на ефективността на мерките. Именно тези елементи се явяват проблемни по делото. Данните по преписката сочат, че резервните копия и базите данни са били съхранявани по начин, който не е гарантирал тяхната независимост от засегнатата инфраструктура, поради което и самите резервни копия са били компрометирани при атаката. Не са представени убедителни доказателства за периодични тестове, за вътрешен или външен одит преди инцидента, нито за актуализирана оценка на риска след 2019 г., въпреки твърденията на администратора за последващо преразглеждане през 2021 г. и 2023 г. При обработването на здравни данни от лечебно заведение тези пропуски не могат да бъдат счетени за несъществени, тъй като именно възможността за надеждно възстановяване на данните при технически инцидент е част от дължимото ниво на сигурност.

Неоснователно е обаче решението на административния орган в частта, в която при определяне на тежестта на нарушението е отчетено и вероятно компрометиране на поверителността на данните, без това да е установено по достатъчно категоричен начин. Съдът приема, че по делото не са събрани доказателства за реално осъществено изтичане, копиране, разпространение или предоставяне на лични данни на трети лица. Наличието на ransomware атака и неоторизиран достъп до информационната среда обосновават извод за сериозен риск и за нарушение на сигурността в аспекта на наличността, но не са достатъчни сами по себе си, за да се приеме като доказан факт и нарушение на поверителността чрез ексфилтрация на данни.

Този извод се подкрепя от приетата съдебно компютърно-техническа експертиза. Макар заключението да следва да се цени с оглед направените от вещото лице уточнения относно липсата на достъп до първичните машини и непълнотата на запазените логове, то не установява данни за трансфер на лични данни извън системата на жалбоподателя. Напротив, вещото лице е посочило, че трансфер на приблизително 10 TB данни в рамките на установения времеви интервал е технически невъзможен. При тези данни съдът приема, че административният орган е могъл да отчете наличие на висок риск, но не и да третира като настъпила фактическа последица компрометиране на поверителността чрез изтичане на данни. Вероятността за такова нарушение има значение при оценката на риска и при преценката за необходимите коригиращи мерки, но при определяне на имуществената санкция по чл. 83 от Регламента следва да се изхожда от установените, а не от предполагаемите последици.

Поради това съдът намира, че решението е законосъобразно в частта, в която е прието, че е налице нарушение на сигурността на личните данни, свързано с компрометиране на тяхната наличност и с недостатъчност на въведените от администратора технически и организационни мерки. Законосъобразни са и дадените разпореждания за регламентиране на периодичен анализ на риска, извършване на периодичен одит, актуализиране на процедурите за архивиране и бекъпи и утвърждаване на документация относно защитата на информационните системи. Тези мерки са пряко свързани с констатираните пропуски и са насочени към привеждане на обработването в съответствие с изискванията на Регламента.

Различен е изводът относно размера на наложената имуществена санкция. Съгласно чл. 83, § 1 от Регламент (ЕС) 2016/679 санкциите следва във всеки конкретен случай да бъдат ефективни,

пропорционални и възпиращи. При определяне на размера им надзорният орган е длъжен да съобрази обстоятелствата по чл. 83, § 2, включително естеството, тежестта и продължителността на нарушението, броя на засегнатите субекти на данни и степента на причинената вреда, дали нарушението е извършено умишлено или по небрежност, действията за смекчаване на последиците, степента на отговорност на администратора с оглед въведените мерки, степента на сътрудничество с надзорния орган, категориите засегнати лични данни, начина, по който нарушението е станало известно на надзорния орган, както и всички други смекчаващи или утежняващи обстоятелства.

В конкретния случай са налице обстоятелства, които обосновават налагане на имуществена санкция. Жалбоподателят е лечебно заведение и обработва здравни данни, които са специална категория лични данни по смисъла на чл. 9 от Регламент (ЕС) 2016/679. Инцидентът е засегнал информационни системи, използвани при осъществяване на медицинска дейност, като е довел до блокиране на достъпа до данни и до затруднение в обичайната работа на лечебното заведение. Установените пропуски относно резервните копия, оценката на риска и периодичния контрол са съществени, тъй като се отнасят до основни елементи от сигурността на обработването.

Наред с това обаче са налице и значими смекчаващи обстоятелства, които не са получили достатъчна тежест при определяне на санкцията. Нарушението не е извършено умишлено. Няма данни за предходни сходни нарушения от страна на администратора. Не се установява реализирана имуществена облага или избегнати разходи като непосредствена цел на поведението му. Жалбоподателят сам е уведомил КЗЛД за нарушението в срока по чл. 33 от Регламента, съдействал е в хода на проверката и е предприел действия за възстановяване на работоспособността на системите. По делото не са установени конкретни вреди за субектите на данни, нито доказано изтичане или разпространение на техни лични данни. Това не елиминира нарушението, но има пряко значение за неговата тежест и за размера на санкцията.

При така установените обстоятелства съдът намира, че наложената имуществена санкция в размер на 100 000 лева е несъразмерна. Този размер не съответства в достатъчна степен на доказания обем на нарушението, доколкото санкцията е определена при фактическа предпоставка за по-висока тежест, а именно вероятно засягане на поверителността на данните, което в съдебното производство не се установи по несъмнен начин. Съдът приема, че санкцията следва

да остане в размер, който отчита сериозността на обработваните данни и пропуските в техническите и организационните мерки, но същевременно съобразява липсата на доказано изтичане, своевременното уведомяване, съдействието и предприетите последващи действия.

С оглед на това съдът намира, че справедлив, пропорционален и възпиращ размер на имуществената санкция е 50 000 лева. Така определеният размер е в рамките на приложимия по чл. 83, § 5, б. „а“ от Регламента максимум, но същевременно съответства на действително установеното нарушение, което се изразява в компрометиране на наличността и недостатъчност на мерките, без доказано изтичане на данни. Този размер е достатъчен да изпълни превантивната и санкционната функция на чл. 83 от Регламент (ЕС) 2016/679, без да надхвърля необходимото за постигане на целите на Регламента при конкретно установените факти.

По изложените съображения жалбата следва да бъде уважена частично, като оспореното решение бъде изменено в частта относно размера на наложената имуществена санкция, която следва да бъде намалена от 51 129.19 евро (100 000 лева) на 25 564.59 евро (50 000 лева). В останалата част жалбата следва да бъде отхвърлена.

Предвид изхода на делото следва да се постави на обсъждане претенцията за разноски на двете страни.

Претенцията за разноски на жалбоподателя е частично основателна съразмерно на уважената част на жалбата, на основание чл. 143, ал.1 от АПК във връзка с чл. 78, ал.1 от ГПК и чл. 144 от АПК. Материалният интерес по делото е 100 000 лв. Уважената част е в размер на 50 000лв., а отхвърлената – в размер на 50 000лв. По делото са представени доказателства за направени разноски в размер на 4671,31 евро, от които 25,56 евро за държавна такса, 3 067,75 евро за адвокатско възнаграждение и 1 578 евро за вещо лице. Съразмерно на уважената част от жалбата, КЗЛД дължи плащане на разноски на жалбоподателя в размер на 2335.65 евро. Съдът намира, че предвид материалния интерес по делото и фактическата сложност уговореното възнаграждение не е прекомерно.

Претенцията за разноски на процесуалния представител на КЗЛД също е частично основателна, съразмерно на отхвърлената част на жалбата, на основание чл. 143, ал. 3 от АПК във вр. с чл. 78, ал. 3 от ГПК и чл. 144 от АПК. Съгласно чл. 37. (1) от ЗПП заплащането на правната помощ е

съобразно вида и количеството на извършената дейност и се определя в наредба на Министерския съвет по предложение на НБПП. На основание чл. 25, ал.1 от Наредбата за заплащането на правната помощ, съдът определя възнаграждение на процесуалния представител на КЗЛД по делото в размер на 230.08 евро (450лв.). Съразмерно на отхвърлената част на жалбата, жалбоподателят дължи на КЗЛД разноски в размер на 115.04 евро.

По компенсация КЗЛД следва да бъде осъдена да плати на жалбоподателя разноски в размер на 2220.61 евро

Водим от горното, съдът

Р Е Ш И:

ИЗМЕНЯ Решение № ПАИКД-13-15/2024 г. от 15.09.2025 г. на Комисията за защита на личните данни в частта, с която на „Специализирана очна болница за активно лечение „Вижън“ ЕООД е наложена имуществена санкция в размер на 100 000 лева за нарушение на чл. 5, § 1, б. „е“ във връзка с чл. 32, § 1, б. „б“ и б. „г“ и чл. 5, § 2 от Регламент (ЕС) 2016/679, като ОПРЕДЕЛЯ размера на имуществената санкция на 25 564.59 евро (50 000 лева).

ОТХВЪРЛЯ жалбата на Специализирана очна болница за активно лечение „Вижън“ ЕООД срещу Решение № ПАИКД-13-15/2024 г. от 15.09.2025 г. на Комисията за защита на личните данни в останалата част.

ОСЪЖДА Комисията за защита на личните данни да заплати на „Специализирана очна болница за активно лечение „Вижън“ ЕООД разноски по делото в размер на 2220.61 евро.

Решението подлежи на обжалване пред Върховния административен съд в 14-дневен срок от съобщаването му на страните.