# Р Е Ш Е Н И Е
**№ 20284**

гр. София, 22.05.2026 г.

**В ИМЕТО НА НАРОДА**

**АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД**, **Второ отделение 24 състав,** в публично заседание на 01.04.2026 г. в следния състав:

**СЪДИЯ: Анастасия Хитова**

при участието на секретаря Анжела Савова, като разгледа дело номер **1573** по описа за **2026** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145 и следващите от Административнопроцесуалния кодекс /АПК/ вр. с чл. 84, ал. 2 от Закона за защита на личните данни /ЗЗЛД/ .
Образувано е по жалба на „Стоун Компютърс“ АД, със седалище и адрес на управление: [населено място], [улица], чрез адвокат Д. Ч., САК, със съдебен адрес: [населено място], [улица], срещу Решение № ПАИКД-13-1/2025 г. от 05.01.2026 г., постановено от Комисия за защита на личните данни /КЗЛД/. В жалбата са изложени съображения за незаконосъобразност на оспореното решение, поради несъответствие с материалния закон и при допуснати съществени нарушения на административнопроизводствените правила.
В съдебно заседание жалбоподателят „Стоун Компютърс“ АД се представлява от адвокат Ч., която поддържа жалбата. Претендира присъждане на разноски, съгласно представен списък по чл. 78 от ГПК вр. чл. 144 от АПК.
Ответникът – Комисия за защита на личните данни, в съдебно заседание се представлява от юрисконсулт Г. и юрисконсулт Я., които молят съда да отхвърли депозираната жалба като неоснователна. Претендира се присъждане на юрисконсултско възнаграждение. Представено е писмено становище.
Административен съд София град, 24 състав след като обсъди доводите на страните и прецени представените по делото доказателства, приема за установено от фактическа страна следното:
Административното производство в КЗЛД е образувано във връзка с постъпило Уведомление с вх. № ПАИКД-13-1/02.01.2025 г. за нарушение на сигурността на личните данни по чл. 33 от Регламент /ЕС/ № 2016/679, подадено от „Стоун Компютърс“ АД /л.14/. В уведомлението се

съобщава за осъществена масирана хакерска атака по отношение на „Стоун Компютърс“ АД на 01.01.2025 г., в резултат на което данни на клиенти на дружеството са криптирани. Посочено е, че към датата на подаване на уведомлението не е установено изтичане на данни, респективно са предприети мерки за ограничаване на причинените щети.
От КЗЛД до „Стоун Компютърс“ АД е изпратено Писмо с рег. № ПАИКД-13-1#1/10.01.2025 г., с което е изискана информация и доказателства за изясняване на фактите и обстоятелствата във връзка с полученото уведомление /л.15/.
Постъпил е отговор от „Стоун Компютърс“ АД с вх. № ПАИКД-13-1#2/17.01.2025 г., с който е предоставена информация и документи по запитването на КЗЛД /л.16-444, т.I, л.445-628, т.II/. В тази връзка за случая е изготвена Докладна записка с рег. № ПАИКД-13-#3/27.01.2025 г., разгледана на заседание на КЗЛД на 29.01.2025 г.
От КЗЛД до „Стоун Компютърс“ АД е изпратено Писмо с рег. № ПАИКД-13-1#6/24.04.2025 г., с което дружеството е уведомено, че подаденото от него уведомление е разгледано на заседание на КЗЛД, проведено на 29.01.2025 г. и обективирано в Протокол № 4, като с оглед констатиран риск за правата на засегнатите субекти на данни е взето решение за извършване проверка на място. /л. 629, т.II/.
С Писмо рег. № ПАИКД-13-1#7/12.09.2025 г. на КЗЛД „Стоун Компютърс“ АД е уведомено за откриване процедура по извършване на проверка по случая. Към уведомлението за проверка е приложен и Въпросник за проверка /л. 630-633, т.II/. С Писмо вх. № ПАИКД-13-1#8/17.09.2025 г., от страна на администратора на лични данни е поискано удължаване на 10-дневния срок за отговор поради големия обем на информацията /л.634, т.II/.
С Писмо рег. № ПАИКД-13-1#9/19.09.2025 г. на КЗЛД, „Стоун Компютърс“ АД е уведомено, че на 29.09.2025 г. в 13:00 часа ще бъде открита процедура по извършването на проверка на място /л.635, т.II/.
С Писмо вх. № ПАИКД-13-1#11/25.09.2025 г. на „Стоун Компютърс“ АД до КЗЛД е изпратена изисканата информация, а именно попълнен въпросник и доказателства към него /л. 637-660, т.II/.
От „Стоун Компютърс“ АД с Писмо рег. № ПАИКД-13-1#14/10.10.2025 г. на КЗЛД е изискано да представи допълнителна информация. В указания срок дружеството е представило същата /л. 661-664, т.II/.
В хода на административното производство с Писмо рег. № ДП 58/25 ОТ 09.10.2025 г. на Главна дирекция „Борба с организираната престъпност“ – МВР /ГДБОП-МВР/, КЗЛД е уведомена, че по случая е образувано ДП № 58/2025 г. по описа на ГДБОП-МВР, пр.пр. № 311/2025 г. по описа на Софийска градска прокуратура, както и че разследването не е приключило и поради тази причина не могат да се представят материали от ДП без надлежно разрешение на наблюдаващия прокурор /л. 665, т.II/.
От „Стоун Компютърс“ АД в хода на проверката с Писмо рег. № ПАИКД-13-1#17/16.10.2025 г. и Писмо рег. № ПАИКД-13-1#18/13.11.2025 г. са представени допълнителни документи към образуваната преписка /л. 666-914, т.II, л. 915-1265, т.III/.
Проверката на място е открита на 29.09.2025 г. на място в офиса на „Стоун Компютърс“ АД, чрез връчване заповедта за извършване на проверка на изпълнителния му директор, като са разяснени задачите и начина на нейното протичане, обсъдени са данните и обстоятелствата относно случая, включително предприетите от дружеството мерки за защита на данните и отстраняване уязвимостите, и укрепване на сигурността с цел предотвратяване на бъдещи инциденти. Резултатите от проверката са обективирани в двустранен констативен протокол, неразделна част от констативния акт, в който подробно са описани всички извършени действия и събрани доказателства по случая.

Обобщените резултати от проверката се изразяват в следното:
1. Действително възникнало събитие в „Стоун Компютърс“ АД, 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 нерегламентиран достъп до cloud инфраструктурата на „Стоун Компютърс“ АД, вследствие на което са криптирани записи на лични данни на клиенти на дружеството;
2. Част от производствените данни са криптирани във файлове с невъзможен достъп, архивните файлове са направени неизползваеми чрез криптиране на ниво операционна система с помощта на BitLocker, открита е бележка /Readme.txt/ от страна на атакуващите, потвърждаваща, че се касае за атака от вида рансъмуер;
3. Цялостното възстановяване на засегнатите данни е осъществено до края на м. Февруари 2025 г., като към момента на проверката няма достъп до цялата инфраструктура на „Стоун Компютърс“ АД, предвид, че е изолирана от органите на МВР и СГП, поради образувано досъдебно производство по случая;
4. Въз основа на представените документи „Стоун Компютърс“ АД не определя целите и средствата като администратор, явява се обработващ по смисъла на Регламент /ЕС/ № 2016/679. В случая „Стоун Компютърс“ АД е доставчик на облачна инфраструктура, съхранява данни на свои клиенти, и не определя целите и средствата на обработката. Отношенията между страните са регламентирани със сключен договор за облачна услуга, като „Стоун Компютърс“ АД не е приложил подходящите технически и организационни мерки, вследствие на което:
4.1. системите за сигурност на „Стоун Компютърс“ АД не са реагирали, и по този начин не е осигурено своевременно информиране за настъпил нерегламентиран достъп до облачната среда;
4.2. от дружеството не е извършена редовна преценка и оценка на ефективността на техническите и организационните мерки, тяхното задължително прилагане с оглед гаранция на сигурността на обработването;
4.3. от инцидента са засегнати 71 клиента на „Стоун Компютърс“ АД, при част от които е настъпила загуба на наличност, представляваща съществено въздействие върху техните права и интереси;
4.4. „Стоун Компютърс“ АД не е изпълнило поетите договорни задължения за защита на облачната инфраструктурата и осигуряване на достъп до информацията на клиента и това неизпълнение е причината за пряка загуба на данни. Настъпилият инцидент е нарушил способността за гарантиране на постоянна цялостност и поверителност на процесите по обработване. Установено е, че личните данни не са обработвани с подходящото ниво на сигурност, респективно липса на предприети технически и организационни мерки, осигуряващи защита от прекратяване на достъпа и загуба на наличност;
4.5. образувано досъдебно производство по случая за неправомерен достъп, обосноваващо наличието на нарушение на сигурността по смисъла на Регламент /ЕС/ № 2016/679;
5. Засегнати са следните категории лични данни и информация за 645 576 физически лица – ЕГН, паспортни данни, месторождение, размер на трудово възнаграждение, длъжност и др.
Проверяващият екип установява, че администраторът на лични данни е извършил оценка на риска след инцидента – актуализирана оценка и третиране на информационните рискове от 29.07.2025 г., както и извършен анализ на риска при обработването на лични данни от 2024 г. преди нарушението и е направен извод, че от страна на „Стоун Компютърс“ АД не е извършена редовна преценка и оценка на ефективността на организационните и технически мерки, задължителното им приложение с цел гаранция за сигурност на обработваните данни. Прието е въз основа на представените Доклад на инциденти по сигурността от 25.01.2025 г. и Доклад от

извършените пенетрейшън тестове към информационната инфраструктура на „Стоун Компютърс“ АД от 15.04.2025 г., че липсата на критични пробиви по време на тестовете не отменя необходимостта от регулярен контрол, одит, подобрения, предвид постоянно променящия се ландшафт на заплахите. В тази връзка е направен 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. Посочено е, 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.
В заключение е направен извод, че системите за сигурност на „Стоун Компютърс“ АД не са успели да осигурят своевременно информиране за настъпил нерегламентиран достъп до облачната среда и с това е нарушен чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент /ЕС/ № 2016/676.
На свое заседание, проведено на 20.11.2025 г., КЗЛД е взела единодушно решение за налагане на административно наказание „имуществена санкция“ на основание чл. 58, § 2, б. „и“ от Регламент /ЕС/ № 2016/676 /л.1297-1299, т.III/.
Въз основа на така проведеното административно производство е издадено оспореното решение, с което на основание чл. 58, § 2, б. „и“ вр. чл. 83, § 4, б. „а“ за нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент /ЕС/ № 2016/679 на администратора на лични данни наложено административно наказание - имуществена санкция в размер на 10 000.00 лева.
При така установената фактическа обстановка и доказателства, съдът достигна до следните правни изводи:
Жалбата срещу Решение № ПАИКД-13-1/2025 г. от 05.01.2026 г., издадено от КЗЛД е процесуално допустима, като подадена срещу акт, който подлежи на съдебен контрол, в преклузивния срок за оспорване, от лице, което е адресат на административния акт и чиято правна сфера актът засяга негативно.
Разгледана по същество, жалбата е неоснователна:
Решение е постановено от КЗЛФД в рамките на нейната компетентност, регламентирана в чл. 63 от Правилник за дейността на КЗЛД и на нейната администрация /Правилника/. Оспореният административен акт е издаден от компетентен орган в законен състав и с мнозинство съгласно чл. 9, ал. 3 от ЗЗЛД, в предвидената от закона писмена форма, съгласно чл. 59 от АПК, съдържайки изискуемите реквизити, посочени в чл. 59, ал. 2 от АПК. При издаване на оспорения административен акт не са допуснати съществени административно-процесуални нарушения, които да са самостоятелно основание за неговата отмяна. Противно на релевираните в жалбата доводи, административният орган е съобразил изводите си изцяло със събраните в хода на проверката информация и доказателства след извършен детайлен и подробен анализ.
Съгласно чл. 62, ал. 2, т. 2 от Правилника, след постъпване в КЗЛД на уведомление за нарушение на сигурността на личните данни уведомлението се разпределя на дирекция „Правно-аналитична, информационна и контролна дейност“, която извършва следните действия: б) естеството на нарушението на сигурността на личните данни при отчитане на категориите субекти на данни и записи на лични данни, приблизителният брой на засегнатите субекти на данни и записи на данни, евентуалните последици от нарушението на сигурността и предприетите или предложени от администратора мерки; в) определяне нивото на риска съобразно приета от комисията методика. Безспорно е, че тези действия са осъществени от административния орган след постъпване на уведомлението за нарушение. Съгласно чл. 63, ал. 1 от Правилника, незабавно след събиране на информацията и извършване на анализа по чл. 62, ал. 2, но не по-късно от два месеца

от постъпване на уведомлението за нарушението дирекция „Правно-аналитична, информационна и контролна дейност“ изготвя мотивиран доклад до КЗЛД с предложения, в т.ч. за извършване на проверка по документи или на място, съобразно предложеното ниво на риск. За решението на комисията се уведомява администраторът, а при необходимост и други, свързани с нарушението, страни.

След постъпване на уведомлението за нарушение на сигурността на личните данни по чл. 33 от Регламент /ЕС/ № 2016/679 е извършена проверка на основание чл. 12, ал. 4 от ЗЗЛД в дружеството- администратор на лични данни. Проведено заседание на КЗЛД, която се е произнесла с решение, взето с мнозинство.

КЗЛД като надзорен орган със специална компетентност разполага с правомощията по чл. 58 от ОРЗД във всички случаи, не само когато е сезирана със жалба от засегнати субекти на лични данни. Подаването на уведомление по чл. 33 от ОРЗД е в изпълнение на задължение на администратора на лични данни, но то по никакъв начин не ограничава правомощията на комисията, която дължи пълна проверка на всички обстоятелства в хода на образуваното административно производство. При установено нарушение при обработването на лични данни, обект на защита е не само всеки засегнат субект на лични данни, но и обществените отношения по защита на личните данни като цяло.

По отношение на приложението на материалния закон, настоящият съдебен състав намира следното:

Съгласно чл. 4, § 1, от Регламент /ЕС/ № 2016/679, „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. Според чл. 4, § 2 от Регламент /ЕС/ № 2016/679 „обработване“ на лични данни е 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. Според чл. 4, § 7 от Регламент /ЕС/ № 2016/679 „администратор“ на лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с друг определя целите и средствата за обработване на лични данни, когато целите и средствата за това обработване се определя от правото на съюза или правото на държавата членка.

Не спорно по делото, че „Стоун Компютърс“ АД е администратор на лични данни. Не е спорно от доказателствата по делото, че на дата 01.01.2025 г. срещу „Стоун Компютърс“ АД е проведена масирана хакерска атака тип „Ransomware“, довела до криптиране на лични данни на клиенти на дружеството. В случая е установено, че са засегнати основни и чувствителни данни – имена, ЕГН, адрес, паспортни данни, телефонен номер, имейл адрес, номер на банкова сметка, данни за сключени застраховки и др. на 645 576 физически лица.

Спорът между страните е правен, състои се в това дали „Стоун Компютърс“ АД е осъществило състава на вмененото му нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент /ЕС/ № 2016/679.

При установено нарушение на сигурността на личните данни за администратора

възникват редица задължения по силата на Регламент /ЕС/ № 2016/679. Сред тях е и задължението по чл. 33, § 1 от Регламента, а именно: без ненужно забавяне и когато това е осъществимо - не по-късно от 72 часа след като е разбрал за нарушението да уведоми надзорния орган, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа. Безспорно такова уведомление от жалбоподателя е направено в законоустановения срок от 72 часа.

От страна на КЗЛД на „Стоун Компютърс“ АД за установеното нарушение е наложена имуществена санкция в размер на на 10 000.00 лева за нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент /ЕС/ № 2016/679, като размерът на наказанието е определен на основание чл. 83, § 4, б. „а“.

Съгласно чл. 5, § 1 от Регламент /ЕС/ № 2016/679, личните данни следва да са обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните /„законосъобразност, добросъвестност и прозрачност“/; да се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели /„ограничение на целите“/; да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват /„свеждане на данните до минимум“/; да са точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват /„точност“/; да са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните /„ограничение на съхранението“/; да са обработвани 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 /„цялостност и поверителност“/.

В чл. 5, § 2 от Регламент /ЕС/ № 2016/679 е установен принципът за отчетност, а именно, че администраторът на лични данни носи отговорност и следва да е в

състояние - във всеки момент, да докаже - при обработване личните данни на физическото лице, спазване на принципите, закрепени в чл. 5, § 1.
Разпоредбата на чл. 32, § 1, буква „б“ гласи, че 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: б. „б“ - способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване и б. „г“ - процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.  В параграф 2 от същия член от Регламент /ЕС/ 2016/679 е посочено, че 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.
Възприемането на тезата на Комисията, която се налага от процесното решение, че при осъществен неправомерен достъп до данните, винаги е налице нарушение на чл. 32, § 1 от ОРЗД, означава да се приеме, че всеки който е станал обект на каквото и да е посегателство, следва да понесе отговорност, че е допуснал осъществяването на същото, независимо, че може да е взел всички възможни към този момент технически и организационни мерки за защита на данните. Именно, за да не се допусне това, Комисията дължи изследване и преценка на съществуващите до нарушението мерки за защита на данните и преценка дали те са били подходящи и съобразени с 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“. Следователно, за да се приеме, че е налице нарушение на чл. 32, § 1 и § 2 от Регламента, е необходимо да се изследват и анализират мерките, които вече са били предприети за гарантиране защитата на личните данни към момента на осъществяване на посегателството върху лични данни, като се проучат и анализират техническите параметри и характеристики на съществуващите системи, както и какви организационни мерки за защита на данните са съществували и до каква степен те са били подходящи, „само по този начин, ще са гарантирани както правата на субекта на данните, така и правата на администраторите на лични данни- Решение № 8668/07.10.2022 г., постановено по административно дело № 3441/2022 г. по описа на ВАС.
В тази връзка следва да се имат предвид и разясненията, дадени в решение от

14.12.2023 г. на трети състав на СЕС по дело № C-340/2021 г., че чл. 24 и 32 от Регламент /ЕС/ № 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО /Общ регламент относно защитата на данните/, трябва да се тълкуват в смисъл, че „неразрешено разкриване на лични данни или неразрешен достъп до такива данни от „трета страна“ по смисъла на член 4, точка 10 от този регламент сами по себе си не са достатъчни, за да се приеме, че приложените от съответния администратор технически и организационни мерки не са „подходящи“. Чл. 32 от Регламент 2016/679 трябва да се тълкува в смисъл, че „преценката дали приложените от администратора технически и организационни мерки по този член са подходящи трябва да бъде направена от националните юрисдикции конкретно, като се вземат предвид рисковете, свързани със съответното обработване, и като се прецени дали естеството, обхватът и прилагането на тези мерки са съобразени с тези рискове“. Принципът на отчетност на администратора, закрепен в чл. 5, § 2 и конкретизиран в чл. 24 от Регламент 2016/679, трябва да се тълкува в смисъл, че „в исково производство за обезщетение, администраторът носи тежестта за доказване на обстоятелството, че приложените от него мерки за сигурност по чл. 32 са подходящи“. Следва да се има предвид и, че „администраторът не се освобождава от задължението си по член 82, параграфи 1 и 2 за обезщетяване на претърпените от дадено лице вреди само поради факта, че тези вреди произтичат от неразрешено разкриване на лични данни или неразрешен достъп до такива данни от „трета страна“ по смисъла на член 4, точка 10 от посочения регламент“.

В мотивите на оспореното решение от КЗЛД е посочено, че „Стоун Компютърс“ АД в качеството си на обработващ лични данни не е извършил редовна преценка и оценка на ефективността на техническите и организационни мерки, тяхното задължително прилагане с оглед гаранция на сигурността на обработването. Това е довело до невъзможността „Стоун Компютърс“ АД да приложи подходящи мерки, в резултат на което е осъществен неоторизиран достъп до данните, впоследствие изцяло ограничен. Прието е, че именно това е причината за реализиране на нарушението, довело до загуба на личните данни на 645 576 физически лица. В тази връзка Комисията е предприела действия за установяване изпълнил ли е администраторът тези свои задължения. Следва да се отбележи, че в съображение 83 от Регламента е посочено, че с цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на настоящия регламент, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо

рисковете и естеството на личните данни, които трябва да бъдат защитени. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, материални или нематериални вреди.
В процесния случай както се установи по делото в хода на проведеното административно производство от страна на „Стоун Компютърс“ АД са представени доказателства за изготвена оценка на риска за сигурността на данните преди възникването на инцидента, включително и такава изготвена след извършване на нарушението, включително и други документи относно предприетите технически и организационни мерки за защита. Всички те са обсъдени от административния орган детайлно и подробно, като е направен извод, че въпреки предприетите технически и организационни мерки, предвидени в договорите за предоставяне на облачни услуги, същите са се оказали недостатъчни, поради което трета страна е извършила неоторизиран достъп до лични данни, обработвани от различните администратори – клиенти. Обоснован се явява изводът на административния орган, че системите за сигурност на „Стоун Компютърс“ АД не са успели да осигурят своевременно информиране за настъпил нерегламентиран достъп на облачната среда, което е в нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент (ЕС) 2016/679. Поради това съдът намира за правилно ангажирана отговорността на администратора на лични данни за нарушение на чл. 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент /ЕС/ № 2016/679, като са взети предвид смекчаващите и утежняващи фактори.
За констатираното нарушение на основание чл. 58, параграф 2, буква „и“ от Регламент /ЕС/ № 2016/679 на „Стоун Компютърс“ АД е наложено наказание - имуществена санкция в общ размер на 10 000.00 лева, съгласно 83, § 4, б. „а“ за нарушение на 5, § 1, б. „е“ вр. чл. 32, § 1, б. „б“ от Регламент /ЕС/ № 2016/679.
Според чл. 83, § 4, б. „а“ ОРЗД, Нарушенията на посочените по-долу разпоредби подлежат, в съответствие с параграф 2, на административно наказание „глоба“ или „имуществена санкция“ в размер до 10 000 000 EUR или, в случай на предприятие — до 2 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока: а) задълженията на администратора и обработващия лични данни съгласно членове 8, 11, 25—39 и 42 и 43 .
В конкретния случай от страна на КЗЛД при определяне размер на наложената санкция правилно е взет ГФО на „Стоун Компютърс“ АД за финансовата 2025 г., съгласно който към датата на провеждане на заседанието на КЗЛД – 20.11.2025 г. е с посочен оборот на дружеството в размер или 21 122.00 лв. Цитираната по горе разпоредбата е със санкционен характер, поради което императивното правило за включването на параметъра „процент от годишен световен оборот за предходната

финансова година на предприятието“ при определяне размера на санкцията, трябва да бъде съобразено и приложено недвусмислено от съответния надзорен орган. В случая съгласно дадените правомощия на административния орган с разпоредбата на чл. 58, §1, б. „а“, „б“, „д“ и „е“ от ОРЗД, КЗЛД правилно е определила размера на имуществената санкция съобразно последно публикувания в Търговски регистър, Агенция по вписвания ГФО за 2025 г. Доводите на жалбоподателя за незаконосъобразно определяне размера на имуществената санкция са неоснователни и недоказани. Също така следва да се има предвид, че към момента на налагане на имуществената санкция от страна на административния орган са взети предвид и смекчаващите отговорността обстоятелства, а именно поведението на „Стоун Компютърс“ АД, предприетите от него действия относно защита на информационните системи.

Съгласно разпоредбата на чл. 83, § 2 от Регламента, когато се взема решение дали да бъде наложено административно наказание „глоба" или „имуществена санкция" и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат следните елементи: а.) естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда; б.) дали нарушението е извършено умишлено или по небрежност; в.) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни; г.) степента на отговорност на администратора или обработващия лични данни като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с членове 25 и 32; д.) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни; е.) степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него; ж.) категориите лични данни, засегнати от нарушението; з.) начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението; и.) когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, посочени в член 58, параграф 2, във връзка със същия предмет на обработването, дали посочените мерки са спазени; й.) придържането към одобрени кодекси на поведение съгласно член 40 или одобрени механизми за сертифициране съгласно член 42; к.) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението. В случая, КЗЛД е определила размера на санкцията като е изследвала и се е водила от всеки един от посочените в чл. 83, § 2 от Регламента критерии.

Предвид гореизложеното, настоящият съдебен състав намира жалбата за

неоснователна, поради което следва да бъде отхвърлена.
С оглед изхода на делото основателна се явява претенцията на ответника за присъждане на разноски за юрисконсултско възнаграждение. Същото е заявено своевременно, поради което на ответника следва да се присъди на основание чл. 143, ал. 1 от АПК вр. чл. 37 от Закон за правната помощ вр. чл. 24, изр. второ от Наредбата за заплащане на правна помощ юрисконсултско възнаграждение в размер на 102.26 евро.
***Така мотивиран и на основание чл. 172, ал. 2, предложение второ, Административен съд София град, 24 състав***,

**Р Е Ш И:**

**ОТХВЪРЛЯ** жалбата на „Стоун Компютърс“ АД срещу Решение № ПАИКД-13-1/2025 г. от 05.01.2026 г., издадено от Комисия за защита на личните данни.
**ОСЪЖДА** „Стоун Компютърс“ АД да заплати на Комисията за защита на личните данни сумата в размер на 102.26 евро, представляваща юрисконсултско възнаграждение.
**РЕШЕНИЕТО подлежи на обжалване с касационна жалба в 14-дневен срок от съобщаването му на страните пред Върховен административен съд на Република България**.

**РЕШЕНИЕТО** да бъде съобщено на страните чрез изпращане на препис от него по реда на чл. 138, ал. 3 във връзка с чл. 137 от АПК.

**СЪДИЯ**: