Р Е Ш Е Н И Е
№ 2204

гр. София, 19.01.2026 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **XXIX КАСАЦИОНЕН СЪСТАВ,** в публично заседание на 28.11.2025 г. в следния състав:

ПРЕДСЕДАТЕЛ: Петя Стоилова
ЧЛЕНОВЕ: Геновева Йончева
Златил Чолаков

при участието на секретаря Милена Чунчева и при участието на прокурора Куман Куманов, като разгледа дело номер **10554** по описа за **2025** година докладвано от съдия Петя Стоилова, и за да се произнесе взе предвид следното:

Производството е по реда на чл.208 и сл. от Административнопроцесуалния кодекс /АПК/ във връзка с чл.63в от Закона за административните нарушения и наказания /ЗАНН/.

С Решение от 07.08.2025г., постановено по НАХД № 14598/2022г. по описа на Софийския районен съд, Наказателно отделение е отменено изцяло Наказателно постановление № 2/23.09.2022г., издадено от В. К. К. - председател на Комисията за защита на личните данни /КЗЛД/, с което на основание чл. 83, § 4, б. „а“ 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/ОРЗД, ОВ Е 119, 4.5.2016, р. 1—88) на „Български пощи“ ЕАД, ЕИК[ЕИК], представлявано Б. Д. Т. - главен изпълнителен директор е наложена „имуществена санкция“ в размер на 1 000 000,00 /един милион/ лева за неизпълнено правно задължение по чл. 32, § 1, б. „б“, „в“ и „г“ и § 2 във вр. с чл. 5, § 1, б. „е“ ОРЗД.

Според касатора решението на първоинстанционния съд е неправилно, поради нарушение на материалния закон, то е немотивирано и необосновано и моли съда да го отмени изцяло. При запознаване с АУАН и НП е видно, че е посочена една и съща дата на извършване на нарушението, а именно - 31.05.2022г. Фиксираната в АУАН и НП дата кореспондира с получено писмо вх. № ПАИКД-13-20#7/31.05.2022г., съдържащо конкретна информация за засегнатите софтуерни продукти и броя засегнати категории лични данни на физически лица. Именно при предоставянето на този документ, КЗЛД по безспорен и категоричен начин установява, че

пробивът в системата на БП е резултатен и че при осъществяване на дейността си „Български пощи“ ЕАД (БП), в качеството на администратор на лични данни съгласно чл. 4, т. 7 от Регламент (ЕС) 2016/679 не е приложило подходящи технически и организационни мерки, в резултат на което е осъществен неоторизиран достъп и неразрешено разкриване на личните данни на физически лица (име, презиме, фамилия; ЕГН/ЛНЧ/служебен номер; адрес: свободен текст, пощенски код, населено място, област; телефон; адрес на електронна поща; финансови данни: заплати, пенсии, парични преводи; информация за здравословното състояние/здравни данни, в т. ч. ТЕЛК/НЕЛК решения).

Според касатора, изводите на първата инстанция се основават единствено на представената по делото експертиза, като фактите се тълкуват едностранно и не в пълен обем, без да се взимат предвид останалите представени доказателства по делото - извършените проверки на място, обективирани в Констативни протоколи, както и приложените към тях документи, разпитът на свидетелите по делото, както и двата доклада от извършения вътрешен одит на дружеството през 2020 и 2021 г., където са посочени рисковете при „Нарушаване на цялостта и поверителността на информацията, вследствие на допускане и необезвреждане на злонамерен софтуер в компютърната мрежа“ и е достигнато до извод: „Приложените контроли снижават риска частично. Необходимо е придобиване на Data Loss Prevention Software и ново техническо решение на системата за абонаменти“. В подкрепа на тезата, че БП не е приложило подходящи технически и организационни мерки, в резултат на което е осъществен неоторизиран достъп е отговорът на вещото лице, което в съдебна зала посочва, че пробивът на системата на БП е могъл да бъде предотвратен, ако са били инсталирани допълнителни софтуерни продукти, които наблюдават й сигнализират за злонамерена активност. Касаторът прави извод, че по отношение предприетите технически и организационни мерки се установява бездействие от страна на администратора, като не са взети предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, изразяващо с в невъвеждането от администратора на подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с регламента. Не са предприети предвидените в чл. 32 от Общия регламент конкретни мерки, а именно: не са взети предвид достиженията на техническия прогрес, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица и не са приложени подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност. В случая въведената система не е била обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност. Нарушението се характеризира с висока обществена опасност – осъществен е неоторизиран достъп до личните данни на физически лица, клиенти на БП, в т. ч. пенсионери, клиенти на контрагенти по сключени договори и служители на БП, съдържащи се в бази данни с приблизително 4 675 393 бр. записи, като базите данни са криптирани, като събитието е получило широк отзвук в обществото. В тази връзка е и определеният размер на санкцията, наложена на „Български пощи“ ЕАД.

В съдебно заседание изложеното в касационната жалба и направеното с нея искане се поддържат чрез юрк.Т., който претендира присъждане на направените в производството разноски в минимален размер за двете инстанции.

Ответникът по касационното оспорване чрез адв. И. и адв. Б. оспорва жалбата и моли да бъде потвърдено първоинстанционното решение като правилно и законосъобразно по съображения, изложени в отговора на касационната жалба. Моли съда да вземе предвид необосноваността на размера на наложената имуществена санкция, тъй като е безспорно установено, че няма изтичане

на никакви лични данни и няма увредени лица от осъществения нерегламентиран достъп. Претендират се разноски по представен списък в размер на 12 918лв.
Представителят на Софийска градска прокуратура - прокурор К. дава заключение за основателност на касационната жалба, споделя изложените доводи от страна на касатора.
Административен съд София-град, XXIX-ти касационен състав, след като се запозна с обжалваното решение и обсъди, както наведените с касационната жалба основания, така и тези по чл.218, ал.2 АПК, намира следното:
Касационната жалба е допустима, като постъпила в законоустановения срок, подадена е от лице – страна в производството и против акт, подлежащ на касационно оспорване.
Разгледана по същество касационната жалба е неоснователна.
След анализ и преценка на събрания по делото доказателствен материал, въззивната инстанция приема за установена следната фактическа обстановка:
„Български пощи“ ЕАД е администратор на лични данни по смисъла на чл. 4, § 7 ОРЛД и обработва лични данни на основание чл. 6, т. 1,6. „а“, „б“, „в“ и „д“ ОРЛД. На 18.04.2022 г. в КЗЛД постъпило уведомление на основание чл. 33 от Регламент (НС) 2016/679 вх. № ПАИКД-13-20/18.04.2022г., допълнено с писмо вх. № ПАИКД-13-20#2/29.04.2022 г., в което е посочено, че на 16.04.2022 г. в 08:30 ч. е установена невъзможност за функциониране на софтуерните приложения в пощенските станции. След проведено обследване е установено, че причината е хакерска атака - пробив на сигурността на информационната инфраструктура посредством специално модифицирана софтуерна платформа, с цел преодоляване на съществуващите технически защити на БП, която е използвана за кражба на пароли, придобиване на контрол и последващо неоторизирано криптиране.
В периода 09.05.2022 г. - 19.05.2022 г. е извършена проверка от КЗЛД и е установена следната хронология на осъществения нерегламентиран достъп и предприетите от БП действия:
От БП разбират за събитието на 16.04.2022 г. в 08:30 ч. при невъзможност за логване в информационните системи от касиерите за раздаване на великденски добавки на пенсионерите, системните администратори разглеждат логовете на сървърите и установяват, че на SQL клъстера, на конто са базите данни, фигурира нерегламентиран администраторски акаунт и голяма част от базите са криптирани в резултат на хакерска атака. Засегнати са сървърни конфигурации на SQL сървърите, като са заразени с ransomware злонамерен софтуер. Криптирани са файловете на базите данни, разположени па виртуалните машини, с разширение: ©Thomas Decription. Нямало установени криптирани данни, разположени на физически отделни сървъри. Извършена е оценка, в съответствие с Инструкция за управление на инциденти, версия 02 от 26.09.2014г.: Значимост и въздействие: Приоритетен код 1 „Критичен“. Незабавно е сформиран кризисен щаб с представители на службите за сигурност на всички доставчици на ИТ услуги и е активиран План за непрекъснаост на сигурността на информацията, версия 4/20.08.2018г., с предвидените процедури за реакция при незаконна външна намеса и с отговорните длъжностни лица. На специалисти от ИТ компания „Telelink“ е предоставен пълен достъп и съдействие в диагностиране и търсене на решение.
Установено е от проверяващия екип на КЗЛД, че външните нападатели не са имали непосредствен физически контакт с информационната система на БП, което предполагало използване на някакви агенти за проникване в нея, преди извършване на вредителските действия. Според тях, в такова качество може да се използва връзката с глобалната мрежа и нейните услуги, поведението на служители на организацията, разпространението на вредителски код и т.н.
В резултат на обстоен одит на информационната инфраструктура е констатиран пробив на сигурността на информационната инфраструктура, посредством зловреден софтуер Mimikatz:

платформа за кражба на пароли. Инструментът Mimikatz представлявал силна платформа за компрометиране на потребителски идентификационни данни, използвана от тестери за проникване и тестване на защитата на крайните точки, както и за незаконна намеса за придобиване на неоторизиран достъп до системите на Windows.
Изяснено било по време на проверката, че е използвана уязвимост в сигурността на Microsoft пощенски сървър, чрез която нападателите придобиват достъп до вътрешна памет на Windows системите. Този инструмент представлявал мощна платформа за компрометиране на потребителски идентификационни данни, използвана от тестери за проникване и етични хакери, за да тестват силата на тяхната защита на крайните точки, но също и от участници в мрежовите заплахи, за да получат неоторизиран достъп до системите на Windows. Зловредният софтуер блокирал потребителите от използване на собствените им информационни системи и криптирал файлове и бази данни, като давал на нападателите контрол над всяка информация, съхранявана на сървърите на БП.
Екипът от експерти извършил пълна инспекция на всички сървъри и работни станции. След диагностиката е установено, че бекъпите на базите данни също са криптирани, което допълнително усложнявало ситуацията. Бекъпите на информационните системи са съхранявани на същите дискови масиви, както и съответните продукционни бази данни.
Видно от предоставената по време на проверката на КЗЛД документация, от извършения мониторинг на графика през защитните стени, за периода 01.04.2022г. - 16.04.2022г. не е установен завишен трафик, различен от нормалния, което водело до извода, че данните не са изтеглени от информационната система (няма разпространение на неправомерно достъпените данни).
В хода на извършените действия от страна на БП по установяване на причините и последствията от неоторизирания достъп и неразрешено разкриване на лични данни са констатирани приблизителен брой на засегнатите физически лица и категориите лични данни. Безспорно са установени основните софтуерни продукти, засегнати от неправомерния достъп, чрез които се осигуряват пощенските услуги и бизнес процеси на дружеството и съдържат лични данни.
От проверяващия екип е констатирано, че в дружеството работят много стари софтуери и морално остарели сървъри и работни станции, които не сработват на последните версии на операционните системи и поради тази причина е предоставена възможност по програма Enterprise Subscription Agreement да се използва всяка по-ниска версия на софтуерните продукти, ако хардуерът не позволява преминаването на нова версия. Поради особеностите на използваните софтуерни решения за нуждите на бизнес процесите в БП, част от същите са написани на език, който се поддържа от по-ниска версия на сървърната операционна система. Поради тази причина се налага да се подържат сървърни конфигурации с по-ниска версия на сървърната операционна система. Всички сървърни операционни системи, съобразно използваната версия, са актуаизирани до последните дефиниции. Органите на КЗЛД е установили, че използваните от БП уеб базирани системи за предоставяни услуги на контрагенти и счетоводство, не са поразени от криптовируса, както и повредените от криптовируса бази данни са с обем, както следва: на базите 2 TB и архив 1 TB.
В резултат от предприетите от страна на БП действия към момента на извършената от КЗЛД проверка е възстановена единствено една информационна система (ИКИС) от направен предишния ден от системния администратор регулярен бекъп, който е бил съхранен на неговия компютър. Информационната система ЕПК с възстановена от файл, получен от НОИ след инцидента (за изплащане на следващите пенсии). Останалите информационни системи са невъзстановими, поради факта, че направените бекъпи за тях са криптирани в резултат на

хакерската атака. Констатирано е, че бекъпите на информационните системи са съхранявани на същите дискови масиви, както и съответните продукционни бази данни, което е в нарушение на правилата и принципите за информационна сигурност. Данните и номенклатурите на част от информационните системи са възстановени частично от съществуващата тестова среда в БП. Всички предоставяни от дружеството услуги са възстановени.
Към момента на проверката не е установено копиране/изтичане на лични данни на субекти от засегнати активи и в БП няма постъпили сигнали и жалби във връзка с възникналия инцидент (няма постъпили и в КЗЛД). От БП посочили, че субектите на данни ще бъдат уведомени, след като се установи по безспорен начин, че има нарушение на лични данни в засегнатите от кибератаката активи.
От събраните в хода на извършената от КЗЛД проверка доказателства и проведените работни срещи със служители на БП и отдел „Киберпрестъпност“ в Главна дирекция „Борба с организираната престъпност“ административните органи приели следния вероятен сценарий за осъществяване на хакерската атака:
В началото на месец април 2022 г., чрез прикачен файл към входящо писмо, е заразен пощенският сървър на БП. След активиране на вируса е инсталиран сканиращ софтуер, следящ за използвани пароли на различни нива (системно и потребителско). След разкриване на администраторска парола е осъществен и достъп до сървърите, чрез акаунт с администраторски права, но различен от използваните от системните администратори. Достъпени са всички виртуални машини във виртуалния клъстер;
В хода на извършената от КЗЛД проверка проверяващият екип констатирал, че при осъществяване на дейността си „Български пощи“ ЕАД, в качеството на администратор на лични данни съгласно чл. 4, т. 7 от Регламент (ЕС) 2016/679, не е предприел следните технически мерки за защита на данните:
1.В БП не са приложени подходящи технически и организационни мерки и в резултат на неоторизирания достъп са криптирани бази данни с приблизително 4 675 393 бр. записи;
2.В резултат на хакерската атака е осъществен нерегламентиран достъп до информационните системи и приложения. От извършения мониторинг на графика през защитните стени за периода 01.04.2022г. – 16.04.2022г. не е установен завишен трафик, различен от нормалния, т. е. не са събрани данни за разпространение на достъпената информация;
3.Липсват политики и процедури за формиране и поддръжка на журнални записи (логове);
4.Не са спазени процедурите и политиките за архивиране/бекъпи на информационните системи. Не се осъществява архивиране на базите данни във вид на дългосрочни архиви и такива на външен носител. Бекъпите и базите данни се съхраняват на същите дискови масиви, както и съответните продукционни бази данни. Същите са криптирани при хакерската атака;
5.Недостатъчен контрол за спазване на процедурата за формиране на потребителско име и парола на ниво администратор на информационните системи, вследствие на което използваните преди инцидента потребителско име и парола на БВ администратора (слаба администраторска парола), като потребителското име включва името на А. М. - ръководител на отдел „Бази данни“).
6.Извършеният годишен одит на информационната система но стандарт 180 27001:2013 касае единствено информационната сигурност. Няма изградена система за проверка па защитата на личните данни и стандартът не е надграден до 180/1ЕС 27701:2019;
7.Не са представени доказателства за извършена оценка на въздействието при идентифициран „висок риск” за всяка една система и предприетите мерки (съгласно одобрен и публикуван на интернет страницата на КЗЛД списък на по чл. 35. § 4 от Регламент (ЕС) 2016/679), в т.ч. при първоначално стартиране на нови информационни системи и приложения. Не е констатирано

наличие на утвърдена методика за оценка на риска/въздействието по смисъла на нормативната база за защита на личните данни.
8.Не са представени доказателства за извършен анализ на риска на системите и операциите по обработването, включващи изготвени правила и функционални задължения за работа на всяка информационна система.
9.Липса на последващ контрол за усвоеното от служителите след приключване на обучението по Регламент (ЕС) 2016/679 и ЗЗЛД;
10.В длъжностните характеристики на служителите няма включени задължения за обработване на лични данни на физически лица при изпълнение на конкретните им служебни задължения. Не са актуализирани длъжностните характеристики с включени клаузи, касаещи обработването на лични данни;
11.При извършения вътрешен одит 2021г. по 180/1ЕС 27001:2013 са констатирани рисковете, със значително завишени стойности в сравнение с 2020 г. и с възможните неблагоприятни последици от тях, а именно „пробиви на системите вследствие на външна намеса и прекъсване на услуги, вследствие на отказ на комуникационни устройства”. Не са предприети бързи и адекватни мерки за защита по отношение на констатираните 2021г. уязвимости, водещи до увеличаване на рисковете;
12.Нарушен е принципът на отчетност - липсват одитни записи на отделните събития и дневници (журнали) за привилегированите потребители. Няма внедрена система за тяхното управление (Privileged Access Management, PAM), с оглед контрол, управление и наблюдение на достъпа до критични активи;
13.Не е внедрена Система за управление и анализ на събитията в областта на сигурността (Security information and event management, SIEM) за осигуряване на анализ в реално време на сигналите за сигурност, генерирани от мрежовия хардуер и приложения;
14.Не се прилагат в пълен обем правилата и процедурите за защита на личните данни от дирекция „Сигурност” и Звено „Зашита на личните данни”. Основните отговорности за работоспособността на информационните системи са съсредоточени в дирекцията „Информационни и комуникационни технологии“;
15.о време на проверката не са събрани доказателства за реализация на Privacy By Design, Privacy By Resign, Privacy By Default, изразяващо се в провеждане на консултации с длъжностното лице по защита на личните данни по отношение на разработване или закупуване на информационна система и оборудване. Не се осъществяват периодични консултации с него с оглед анализа на техническите и организационните мерки за защита на личните данни, обработвани в информационните системи. Представени са единствено документи, в които присъства подписът на длъжностното лице по защита на личните данни за съгласуване, но не и такава с изразено негово експертно мнение;
16.Липсват доказателства за периодична ангажираност на висшия мениджмънт за запознаване с проблемите на информационната сигурност и нейното ресурсно осигуряване;
17.Не са предприети действия за обновяване па операционните системи и на СУБД към актуални версии на Microsoft SQL (версия SQL 2019), поради факта, че някои от използваните приложения няма да работят на по-високи версии. Правени са актуализации до последните дефиниции. Това създава потенциална опасност за сигурността на данните поради изтичане срока за тяхната поддръжка;
18.В сключените договори между администратор и обработващ липсват клаузи относно конкретно задължение за предприемане на технически и организационни мерки при обработване на данните и не са разписани правила за осъществяване на контрол върху въведените мерки за

сигурност;
19.От предоставените правила и процедури за управление на доставчиците не са дефинирани правила и принципи за избор на доставчици, както и такива за оценка на рисковете, свързани с тях. Използват се правилата и изискванията, регламентирани в ЗОП.
Резултатите от проверката са обективирани в констативен акт от 29.06.2022г., изготвен от проверяващия екип. С акт за установяване на административно нарушение № 2/25.07.2022г., съставен от Р. М. К. - началник отдел „Контрол и административнонаказателни производства“ към дирекция „Правни производства и надзор“ при КЗЛД и в присъствието на Т. И. П. и В. Е. Н. - свидетели при установяване на твърдяното нарушение е констатирано, че при осъществяване на дейността си жалбоподателят „Български пощи“ ЕАД, в качеството на администратор на лични данни съгласно чл. 4, т. 7 от Регламент (ЕС) 2016/679, не е приложил подходящи технически и организационни мерки, описани в 19 точки, в резултат на което е осъществен неоторизиран достъп и неразрешено разкриване на личните данни на физически лица (име, презиме, фамилия; ЕГН/ЛНЧ/служебен номер; адрес: свободен текст, пощенски код, населено място, област; телефон; адрес на електронна поща; финансови данни: заплати, пенсии, парични преводи; информация за здравословното състояние/здравни данни, в т. ч. ТЕЛК/НЕЛК решения: за служителите на БП; трудов стаж: за служителите на БП; трудово възнаграждение: за служителите на БП; банкова сметка: за служителите на БП) от информационните бази данни, поддържани от дружеството, като от съдържанието на подаденото на 18.04.2022г. уведомление по чл. 33 от Регламент (ЕС) 2016/679 уведомление съгласно чл. 33 от Регламент (ЕС) 2016/679 с вх. № ПАИКД- 13-20/18.04.2022 г. и от представените на 31.05.2022 г. в КЗЛД документи (писмо вх. № ПАИКД-13-20#7/31.05.2022 г.), с впоследствие коригирани данни е установено, че е осъществен неоторизиран достъп до личните данни на физически лица (клиенти на БП, в т.ч. пенсионери, клиенти на контрагенти по сключени договори и служители на БП), съдържащи се в бази данни с приблизително 4 675 393 бр. записи, като базите данни са криптирани. Повредените от криптовируса бази данни са с обем, както следва: на базите от 2 TB, на архива 1 TB.
В акта е отразено, че в резултат на неправомерния достъп е нарушена способността за гарантиране на постоянна поверителност, наличност, цялостност и устойчивост на системите и услугите за обработане, както и способността за своевременно възстановяване на наличността и достъпа до личните данни, с което е нарушен чл. 32, § 1, букви „б“, „в“ и „г“ и § 2, във връзка с чл. 5, § 1, буква „е“ от Регламент (ЕС) 2016/679, както и че нарушението в установено 31.05.2022 г. в [населено място]. Въз основа на горепосочения акт е издадено атакуваното наказателно постановление № 2/23.09.2022 г. от В. К. К. - председател на КЗЛД, с което на основание чл. 83, § 4, б. „а“ от ОРЗД на „Български пощи“ ЕАД е наложена „имуществена санкция“ в размер на 1 000 000,00 /един милион/ лева, за неизпълнено правно задължение по чл. 32, § 1, б. „б“, „в“ и „г“ и § 2 във вр. с чл. 5, §, 1, б. „е“ ОРЗД.
Въз основа на гореизложеното, въззивният съд е обосновал извод, че в АУАН и НП не е отразена еднозначно датата на твърдяното административно нарушение, като е същата е неясна и енигматична, което представлява самостоятелно формално основание за отмяна на обжалваното наказателно постановление, тъй като води до накърняване на правото на защита на санкционираното лице. По противоречив начин в АУАН и НП е отразена и датата на установяване на процесното нарушение, доколкото от една страна се сочи, че това е сторено на 31.05.2022 г., а от друга - посоченият релевантен факт се обосновава с документи и информация, съдържащи се в получени писма от 01.06.2022 г., 23.06.2022 г. и 24.06.2022 г.
Във връзка със санкционираното неизпълнение на задължението по чл. 32, § 1, б. „б“, „в“ и „г“ и § 2 във вр. с чл. 5, § 1, б. „е“ ОРЗД въззивният съд се е позовал на приетото по делото Заключение

на комплексната съдебна компютърно-техническа и икономическа експертиза, изготвено от вещите лица инж. Д. С. и Р. Ш., като е приел, че административнонаказателното производство по установяване на административното нарушение и по налагане на административно наказание е опорочено, поради допуснати съществени процесуални нарушения, довели до ограничаване правото на защита на въззивника, а отделно от това отговорността на юридическото лице е ангажирана при некоректно приложение на материалния закон.
Решението на СРС е правилно.
Изводите на решаващия съд се споделят изцяло от настоящата инстанция и тя препраща към тях на основание чл.221, ал.2, изр.2-ро АПК. Обжалваното решение е постановено въз основа на събраните доказателства, като съдът е изпълнил задължението си, разглеждайки делото по същество, да установи с допустимите от закона доказателства дали е извършено нарушение, обстоятелствата, при които е извършено, както и законосъобразността на наложеното административно наказание. При субсидиарното прилагане на НПК, районният съд е изпълнил служебното си задължение да проведе съдебното следствие по начин, който е осигурил обективно, всестранно и пълно изясняване на всички обстоятелства, включени в предмета на доказване по конкретното дело, при точното съблюдаване на процесуалните правила, относно събиране, проверка и анализ на доказателствената съвкупност и не е допуснал процесуални нарушения.
Имуществената отговорност на въззивника “Български пощи“ ЕАД е ангажирана за неизпълнено правно задължение по чл. 32, § 1, б. „б“, „в“ и „г“ и § 2 във вр; с чл. 5, § 1, б. „е“ ОРЗД, за което на основание чл. 83, § 4, б. „а“ ОРЗД му е наложена „имуществена санкция“ в размер на 1 000 000,00 /един милион/ лева.
Съгласно изричната разпоредба на чл. 32, § 1, б. „б“, „в“ и „г“ ОРЛД, 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: способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване; способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент; процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването. Видно от чл. 32, § 2 ОРЛД при оценката на пдходящото 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, като от своя страна чл. 5, § 1,6. „е“ ОРЗД предвижда, че личните данни 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“).
Съгласно т. 42 на Решение от 14.12.2023 г. по дело C-340/21 на СЕС, от член 32, параграфи 1 и 2 от ОРЛД следва, че дали такива технически и организационни мерки са подходящи, трябва да се преценява на два етапа. От една страна, следва да се идентифицират рисковете от нарушение на сигурността на личните данни, породени от съответното обработване, и евентуалните последици от тях за правата и свободите на физическите лица. Тази преценка трябва да се осъществява

конкретно, като се отчита степента на вероятност на идентифицираните рискове и тежестта им. От друга страна, следва да се провери дали мерките, приложени от администратора, са съобразени с тези рискове, като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на това обработване.
Във връзка с горното, правилно въззивният съд е преценил, че показанията на свидетелите Ц. Ц. и Р. К. възпроизвеждат дословно фактическите констатации в АУАН, но се опровергават от заключението на назначената на етапа на съдебното следствие комплексна съдебна компютърно-техническа и икономическа експертиза. Предвид, че неразрешеното разкриване на лични данни или неразрешеният достъп до такива данни от „трета страна“ по смисъла на член 4, точка 10 от ОРЛД сами по себе си не са достатъчни, за да се приеме, че приложените от съответния администратор технически и организационни мерки не са „подходящи“ по смисъла на членове 24 и 32, в каквато насока е даденото тълкуване в т. 1 от диспозитива на решение от 14.12.2023 г. по дело C-340/21 на СЕС, фактът на осъществената хакерска атака - пробив на сигурността на информационната инфраструктура посредством специално модифицирана софтуерна платформа, с цел преодоляване на съществуващите технически защити на БП, която е използвана за кражба на пароли, придобиване на контрол и последващо неоторизирано криптиране не е достатъчен, за да се приеме, че приложените от съответния администратор технически и организационни мерки не са „подходящи“ и това представлява осъществено нарушение на чл.32 § 2 ОРЛД. Възприетият от проверяващия екип „вероятен сценарий“ на хакерската атака, визиращ заразяването на пощенския сървър на „Български пощи“ ЕАД чрез прикачен файл към входящо писмо е послужил за преценка дали мерките, приложени от администратора са съобразени с този риск. На тази база е прието, че „Български пощи“ ЕАД в качеството на администратор на лични данни съгласно чл. 4, т. 7 от Регламент (ЕС) 2016/679, не е предприел множество технически мерки за защита на данните, изброени в дълъг списък от 19 точки. Видно от диспозитива на Решение на КЗЛД рег. № ПАИКД -13-20/06.10.2022г., където са дефинирани съответните мерки, преценени от проверяващите органи като „подходящи“, е даден срок за изпълнението им от три месеца до една година, считано от влизане в сила на решението. В тази връзка верни са констатациите на въззивния съд, че датата на нарушението не е посочена ясно. От вещите лица, изготвили съдебната експертиза обаче е установено, че пробивът на информационната сигурност действително е бил осъществен на 15.04.2022г. през пощенския сървър на “Български пощи” ЕАД, като единствената причина за това е деактивирането по предписание на производителя Microsoft на FIP-FS модула, който защитава от спам и злонамерен софтуер. Тези фактически установявания не са обсъдени в АУАН и издаденото, въз основа на него НП, поради което правото на защита на привлеченото към отговорност юридическо лице не може да бъде реализирано по отношение на тях. В АУАН и НП не е изследвано дали деактивираното на процесния модул представлява риск за нарушение на сигурността на личните данни, респективно дали администраторът е предприел нужните действия за неговото минимизиране, чрез прилагане на подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно: способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване; способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент; процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.
Вещото лице С. пояснява, че бездействието при предприемането на която и да било от фиксираните в АУАН и НП технически и организационни мерки, обособени в 19 отделни точки,

не се намира в пряка и непосредствена причинно-следствена връзка с осъществената хакерска атака и не е от естество да предотврати пробива, респективно криптирането на личните данни. Тези мерки обуславят упражняване от страна на надзорния орган на правомощието му по чл. 58, § 2, б. „г“ ОРЗД (Решение № ПАИКД-13-20/22 от 06.10.2022 г. на КЗЛД), но не предпоставят ангажиране на административнонаказателната му отговорност по ЗАНН, тъй като няма как да се прецени, че точно тези изброени в 19те точки мерки в тяхната кумулативност, ако бяха изпълнени от администратора на лични данни към датата на атаката, тя щеше да бъде предотвратена. Това е така, тъй като деактивирането на FIP-FS модула не е било съобразено като конкретно установен риск, и дали са предприети подходящи технически и организационни мерки от администратора съобразно този риск не е изследвано. Срещу самата хакерска атака е противодействано своевременно, видно от констатираното от проверяващите, поради което не са били изтеглени никакви данни от сървърите на дружество.

Твърдените от административнонаказващия орган фактически положения не са безспорно установени, ето защо като е приел, че отговорността на администратора на лични данни е ангажирана незаконосъобразно, СРС е постановил правилно решение, същото не страда от пороците, визирани в касационната жалба, нито от такива, за които касационната инстанция следи служебно и следва да бъда оставено в сила.

С оглед изхода на делото, на касатора се дължи присъждане на разноски, които се претендират в размер на 12 918лв /6604,87евро/ адвокатско възнаграждение, представена е фактура и преводно нареждане. Направено е възражение за прекомерност, което е неоснователно, предвид големия материален интерес по делото.

Водим от горното, Административен съд София-град, XXIX-ти касационен състав,

Р Е Ш И:

ОСТАВЯ В СИЛА Решение от 07.08.2025г., постановено по НАХД № 14598/2022г. по описа на Софийския районен съд, Наказателно отделение.

ОСЪЖДА Комисията за защита на личните данни да заплати на „Български пощи“ ЕАД разноски по делото в размер на 12 918лв /дванадесет хиляди деветстотин и осемнадесет/ лева (6604,87 евро).

РЕШЕНИЕТО е окончателно и не подлежи на обжалване и протест.

Председател:

Членове: