# Р Е Ш Е Н И Е
**№ 26235**

гр. София, 01.08.2025 г.

**В ИМЕТО НА НАРОДА**

**АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД**, **Второ отделение 31 състав,** в публично заседание на 09.06.2025 г. в следния състав:

**СЪДИЯ: Веселина Женаварова**

при участието на секретаря Розалия Радева, като разгледа дело номер **3039** 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 Административно-процесуалния кодекс (АПК), вр. чл.38, ал. 8, вр. с ал. 3 от Закона за защита на личните данни (ЗЗЛД) и чл. 58, § 2, буква „г“ 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).

С Решение №2633/14.03.2025г. по адм.д.№5991/2024г. на ВАС-Пето отделение е отменено решение № 505/18.01.2024 г. по адм.д.№ 9929/2022 г. по описа на Административен съд София- град и е върнато на същия съд за ново разглеждане от друг съдебен състав делото образувано по жалба на „Български пощи“ ЕАД, ЕИК[ЕИК], срещу решение № ПАИКД-13-20/22 от 06.10.2022 г. на Комисията за защита на личните данни /КЗЛД/, с искане да бъде изцяло отменено. С решението на ВАС са дадени задължителни указания при новото разглеждане на делото да бъдат обсъдени всички наведени от жалбоподателя доводи, че: 1. няма законова презумпция за неподходящи технически и организационни мерки, приложени от администратора на лични данни, само на базата на осъществена хакерска атака, 2. липсва "уязвимост" по смисъла на т. 34, пар. 3 от ДР на Закона за киберсигурност като неустойчивост на информационната система, на вътрешния контрол и на процедурите за сигурност и тяхното реализиране, които могат да се използват за деструктивно въздействие на системата, 3.изтичане на лични данни няма, 4. липсва опора в закона на дадените от КЗЛД разпореждания за преодоляване на описани в акта "дефицити", нито има яснота дали хакерската атака би била предотвратена, ако бяха изпълнени посочените в 19 точки мерки, 5. не е изяснен механизма за осъществения пробив, 6.

задължителен набор от технически и организационни мерки по Регламента и по ЗЗЛД няма и част от предписаните мерки са напълно неотносими към осъществения пробив на системите на "Български пощи" ЕАД, а други имат отношение единствено към преодоляване на последиците, но не и към предотвратяване на пробива, 7. Разпореденият за прилагане по т.6 от решението на КЗЛД стандарт ISO 27701:2019 не фигурира в списъка на стандарти в областта на мрежовата и информационната сигурност, представляващ Приложение №1 към Наредбата за минималните изисквания за мрежова и информационна сигурност, 8. Не става ясно по т.5 от решението на какъв регламент са обосновани според КЗЛД процедурите по формиране на потребителско име и парола, по отношение на които се твърди, че има недостатъчен контрол, 9. По т.8 от решението разпореждането е неясно, защото не е конкретизирано за коя част от политиките на Български пощи ЕАД се отнася, 10. По т.10 от решението също не е ясно промените в длъжностните характеристики с какво ще предотвратят занапред подобни инциденти, 11. По т.18 няма конкретизиране на договорите с кои конкретни лица има предвид КЗЛД. Оспорва се и т.19, според която Български пощи ЕАД не са дефинирали правила и принципи за избор на доставчици, както и такива за оценка на рисковете свързани с тях, а вместо това се ползват правилата и изискванията по Закона за обществени поръчки . Оспорват се като кратки и неподходящи сроковете за изпълнение по конкретните мерки по т. 3, 4, т. 6, т. 15 и т. 16. Дадени са указания и АССГ да обсъди всички наведени конкретни оплаквания за незаконосъобразност на решението на КЗЛД в т. 3, 5, 7, 6 и 16; както и да развие мотиви по довода дали КЗЛД е длъжна при констатиран нерегламентиран достъп, да прилага само принудителни административни мерки, които имат за цел да преустановят и предотвратят онова бездействие на администратора на лични данни, което е в причинна връзка с осъществената кибератака на информационни системи на администратора на лични данни, с цел да бъде предотвратен занапред подобен инцидент.

В съдебно заседание жалбоподателят „Български пощи“ ЕАД, чрез юриск.К., поддържа жалбата. Претендира юрисконсултско възнаграждение.

Ответникът – Комисията за защита на личните данни, чрез гл.експерт Я. в съд.з. и в представено от него писмено становище, оспорва жалбата като неоснователна. Претендира юрисконсултско възнаграждение.

Административен съд – София – град, като взе предвид задължителните указания на ВАС, след като обсъди доводите на страните и прецени събраните по делото писмени доказателства и заключението на вещото лице по назначената експертиза, приема за установено от фактическа страна следното:

"Български пощи" ЕАД е администратор на лични данни по смисъла на чл. 4, т.7 от Регламент 2016/679 и обработва данни на физически лица във връзка с предмета си на дейност.

На 16.04.2022 г. е установена невъзможност за функциониране на софтуерните приложения поради криптирана голяма част от база данни в резултат на хакерска атака. В съответствие с разписани правила за поведение в "Инструкция за управление на инциденти", версия 02 от 2014 г., активиран "План за непрекъснатост на сигурността на информацията, версия 4/2018 г.", са предприети поредица от действия. Пробивът на сигурността е извършен посредством зловреден софтуер Mimikatz, платформа за кражба на пароли. Не могат да бъдат възстановени Интегрирана Автоматизирана система за Управление на Търговската дейност, Информационна система Електронен пенсионен картон, Система за автоматизиране на дейностите по предоставяне на пощенски услуги, отговарящи на пазарните потребности и електронна търговия с интегрирана Е-пакет", Единен софтуер за управление и контрол на пощенско-парични преводи, Унифициран софтуер за управление и отчитане на продажбите на стоки в Български пощи, Интегрирана система за работна заплата и управление на човешки

ресурси Aladin, Интегрирана куриерска информационна система, поради криптиране на базата данни и създадените бекъпи. Засегнати са хиляди лица. В решението на КЗЛД са описани предприети мерки за ограничаване на вредните последици, мерки за възстановяване чрез създадената организация за изграждане на нова информационна инфраструктура на Български пощи върху платформа на държавен хибриден частен облак /ДХЧО/, изграждане на нова домейн и сървърна инфраструктура, обобщаване и възстановяване на информацията, на новите инсталирани сървърни конфигурации се инсталира последна версия на антивирусен софтуер Eset Nod 32, който принципно успявал да прихване и карантинира вируси, изградена е физическа свързаност между ДХЧО и съществуващата информационна инфраструктура на "Български пощи" ЕАД. Посочено е, че са предприети действия за изпълнение на оценката на обхвата на въздействие върху всички активи, успоредно с мерките за възстановяване, изпълнение на стартирани мерки за възстановяване на функционалността на ключовите информационни системи на Български пощи. Описани са подробно: 1. предприети от "Български пощи" ЕАД последващи действия и мерки във връзка с рискове за повторна хакерска атака, 2. мерки за повишаване на защитата на инфраструктурата и недопускане на инциденти от подобен характер, 3.обсъдена е организацията на информационната сигурност във водещия документ Регламент за управление на сигурността на информацията, версия 4/2018, отговорностите на съответните длъжностни лица, одобрената през 2020 г. Политика за защита на лични данни, Процедурата ОПУ 07 Вътрешен одит, Политиките за информационна сигурност, планове за действия в случай на аварии, природни бедствия и др. непредвидени обстоятелства. Направени са констатации относно непрекъсваемостта на функционирането на информационните системи и липсата на резервен център за данни поради липса на финансови средства. Посочени са конкретни действия, които трябва да се извършат за възстановяване на нормалното състояние на цялата система и на плана за непрекъснатост. Направени са констатации относно правилата за служителите, имащи отношение към процесите и дейностите по обработка на личните данни, във връзка с управлението на персоналната сигурност. Обсъдени са всички видове тестове на системата. В 19 точки КЗЛД е направила обобщения във връзка с констатациите като: 1.липсата на политики и процедури са формиране и поддръжка на журнални дневници /лог файлове/, 2. неспазени процедури и политики за архивиране /бекъп/ на информационните системи, като не се осъществява архивиране на бази данни във вид на дългосрочни архиви и такива на външен носител, поради което е невъзможно възстановяване на функционирането на информационните системи и база данни, 3.недостатъчен контрол за спазване на процедурата за формиране на потребителско име и парола на ниво администратор на информационните системи, 4. ненадграден стандарт ISO27001/2013 до ISO LEC 27701/ 2019 за проверка защитата на личните данни, 5.липса на извършена оценка на въздействието и идентифициран висок риск за всяка система, 6.липса на доказателства, че утвърдени от "Български пощи" ЕАД политики и процедури са приложени в цялост, 7.липса на последващ контрол след приключило обучение на служители по Регламент 2016/679 и невключени задължения за обработване на лични данни на физически лица при изпълнение на служебни задължения, 8. при констатирани при одит през 2021 г. рискове със значителни завишени стойности не са предприети бързи и адекватни мерки за защита на уязвимости, 9. нарушен е принцип на отчетност поради липса на записи за отделни събития и журнални дневници за привилегировани потребители, 10. Невнедрена Система за управление и анализ на събитията в областта на сигурността за осигуряване на анализ в реално време на сигнали за сигурност, генерирани в мрежовия хардуер и приложения, 11.Основната отговорност за информационните системи е само за Дирекция "ИКТ",но не се прилага защита от дирекция "Сигурност" и Звено "Защита на лични данни", 12. Не се осъществяват периодични консултации с

длъжностно лице по защита на лични данни, 13. Няма доказателства висшият мениджмънт да е периодично ангажиран и запознат с проблемите на информационната сигурност, 14. Няма действия за обновяване на информационните системи и на СУБД към актуалните версии на Microsoft SOL 2019, защото някои от използваните приложения няма да работят на по-високи версии, 15.В сключени договори администратор- обработващ, липсват клаузи за конкретно задължение за предприемане на технически и организационни мерки при обработване на данните и не са разписани правила за контрол, 16. на доставчиците не са дефинирани правила и принципи за избор на доставчици, както и такива за оценки на рискове.

От така констатираните обстоятелства КЗЛД е направила извод ,че не са приложени подходящи технически и организационни мерки, в резултат на което е извършен нерегламентиран достъп до база данни, след което са били криптирани, а от нарушението на сигурността са засегнати приблизително 4 675 393 бр. записи, съдържащи лични данни на физически лица, 1 700 000 субекти на лични данни от ИАСТУД, от които са индивидуализирани 675 393 бр. физически лица. Нарушена е способността за гарантиране на постоянна поверителност, наличност, цялостност и устойчивост на системите и услугите за обработване, както и способността за своевременно възстановяване на наличността и достъпа до лични данни- нарушение на чл. 32, пар.1, б. "б", "в" и "г" и пар. 2 вр. с чл. 5, пар.1, б."е" от Регламент 2016/679. Обосновано е защо се предприемат принудителни административни мерки в рамките на оперативната самостоятелност на КЗЛД по чл. 58, пар. 2 /без тези по б."и"/ от Регламента с цел предотвратяване или преустановяване извършването на нарушение. В случая от "Български пощи" ЕАД се обработват голям обем от лични данни, но поради липсата на адекватни технически и организационни мерки за защита на лични данни администраторът на лични данни не е успял да изпълни задължението си по чл. 32, пар. 1, б. "б" от Регламента, като е допуснал загуба на наличността и устойчивостта на своите системи и услуги. Използват се компютърни конфигурации, за които не се поддържат по- нови версии на операционната система от Windows 7, който вече не се поддържа от съответния доставчик. Това означава, че поради липса на поддръжка на софтуера, не са отчетени нововъзникнали и новооткрити бъгове и заплахи за системите, които стандартно се отстраняват от самия производител и доставчик на софтуера.

Предвид констатациите и в резултат на проверката, като най-целесъобразна мярка е избрана тази по чл. 58, пар.2, б."г" от Регламента, т.е. даване на конкретни разпореждания на администратора, като му се указва и начина, по който следва да се отстранят констатираните нарушенията и да се предотвратят бъдещи такива нарушения.

С оспореното решение, на основание чл. 58, § 2, буква „г“, за нарушение на чл. 32, § 1, букви „б“, „в"' и „г“ и § 2, във връзка с чл. 5, § 1, буква „е“ от Регламент (ЕС) 2016/679, КЗЛД разпорежда на „Български пощи“ ЕАД да предприеме следните технически и организационни мерки със посочените срокове за изпълнението им:

1. Да извърши анализ на риска на системите и операциите по обработване на лични данни, за всяко звено, участващо в бизнес процесите, както и да се разпишат контролни функции на органите по защита на личните данни. Срок за изпълнение - 3 (три) месеца от влизане в сила на решението;
2. Да извърши оценка на въздействието, съгласно чл. 35, § 4 от Регламент (ЕС) 2016/679, за всяка една система при идентифициран „висок риск“ и в съответствие с одобрения и публикуван на интернет страницата на КЗЛД „Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните". Срок за изпълнение - 6 (шест) месеца от влизане в сила на решението;
3. В резултат на извършените анализ и оценка да актуализира процедурата за формиране на

потребителско име и парола за достъп до информационните системи. Със специален режим на формиране на потребителско име и парола за достъп да се ползват администраторите/ служителите с привилегирован достъп до информационни системи и ресурси. Да внедри приложения за предпазване от опити за разкриване на паролите (brute force атаки). Срок за изпълнение - 3 (три) месеца от влизане в сила на решението;

4. В резултат на т. 1, т. 2 и т. 3, да актуализира политиката за защита па личните данни по отношение всяка една информационна система, поддържана от „Български пощи“ ЕАД. Да внедри система за засичане на потенциално опасни файлове получени в „Български пощи“ ЕАД, чрез електронна поща, която да включва като минимум защита от злонамерен софтуер, потенциално нежелани, опасни и подозрителни приложения. Да разработи процедури за тестване на системите за информационна сигурност, включващи тестове за проникване. Срок за изпълнение - 7 (седем) месеца от влизане в сила на решението;

5. Да изготви и утвърди методика за оценка на инциденти в информационната сигурност и защитата на личните данни, с която включително да се въведе процедура, която да регламентира срокове и периодичност за запознаване на висшето ръководство на „Български пощи” ЕАД със състоянието и нововъзникналите проблеми на системата за информационна сигурност. Срок за изпълнение - 3 (три) месеца от влизане в сила на решението;

6. Да въведе политики и процедури за формиране и поддръжка на журнални записи (логове). Да предприеме необходимите действия за създаване на одитни записи на отделните събития и дневници (журнали) за привилегированите потребители, като се внедрят Система за управление на привилегиите на потребителите (Privileged Access Management, PAM) и Система за управление и анализ на събитията, отразени в дневниците (Security information and event management, SIEM). Срок за изпълнение - 6 (шест) месеца от влизане в сила на решението;

7. Във връзка с чл. 32, § 1, б. „в“ от Регламент (ЕС) 2016/679, да изработи конкретна стратегия и политики за нейната реализация, относно изграждане, поддържане и достъп до архивните копия; актуализиране на процедурите и политиките за архивиране/бекъп на информационните системи; въвеждане на архивиране на базите данни във вид на дългосрочни архиви и такива на външен носител, което да позволи надеждно и своевременно възстановяване. Срок за изпълнение - 3 (три) месеца от влизане в сила на решението;

8. Във връзка с чл. 32, нар. 1, б. „б“ от Регламент (ЕС) 2016/679, да осигури постоянна наличност и устойчивост на бизнес процесите, като се определи ключовата информация за всяка информационна система. Срок за изпълнение - 3 (три) месеца от влизане в сила на решението;

9. Да определи критерии, свързани със сигурността и обработването на лични данни при избор на доставчици и да актуализира правилата и процедурите по избора им. Срок за изпълнение - 4 (четири) месеца от влизане в сила на решението

10. Да актуализира договорите с доставчиците на информационни услуги (инфраструктура и софтуер) за отговорностите им при изграждане на системата за информационна сигурност. Срок за изпълнение - 6 (шест) месеца от влизане в сила на решението.

11. Да актуализира длъжностните характеристики на служителите на „Български пощи" ЕАД с включени клаузи, касаещи обработването на лични данни. Срок за изпълнение - 6 (шест) месеца от влизане в сила на решението;

12. Да допълни и/или измени съдържанието на длъжностната характеристика на длъжностното лице по защита на данните, като се впишат ясни правила и задължения за осъществяване на дейността и контролните му функции. Да въведе задължение длъжностното лице по защита на данните да докладва, освен на изпълнителния директор, и на Съвета на директорите на „Български пощи” ЕАД въпросите, свързани с обработването на лични данни, с

цел постигане обективност на представяната на Съвета информация. Срок за изпълнение - 3 (три) месеца от влизане в сила на решението;

13. Да въведе и приложи механизми за последващ контрол на ефективността на проведените обучения на служителите по защита на личните данни. Срок за изпълнение - 1 (една) година от влизане в сила на решението;

14. Да актуализира договорите/правните актове за възлагане на обработване между администратор и обработващ по смисъла на чл. 28 от Регламент (ЕС) 2016/679. като в тях задължително да се включват техническите и организационни мерки при обработване на лични данни, както и съответните правила за контрол по спазването им. Тези изисквания да се въвеждат и при сключване на нови подобни договори/правни актове. Срок за изпълнение - 6 (шест) месеца от влизане в сила на решението;

15. Съгласно приетите инвестиционни проекти от „Български пощи" ЕАД, да бъдат въведени установените политики и конкретни мерки за защита на личните данни, предложени с извършения през 2021 г. одит съобразно ISO/IEC 27001:2013 в сроковете, съгласно приетите инвестиционни проекти. Срок на изпълнение – до края на 2023г.;

16. Да предприеме действия, при необходимост от замяна на съществуващ хардуер, за обновяване на операционните системи и на системите за управление на бази данни, като се използват само такива, които официално се поддържат от съответните доставчици (вендори). Срок за изпълнение - 1 (една) година от влизане в сила на решението.

Съгласно заключението на вещото лице инж. Д.С. по назначената по делото съдебна компютърна техническа експертиза (СКТЕ), причината за нерегламентирания достъп е деактивирането, по предписание на Microsoft, на важен модул, който защитава от спам и зловреден софтуер. Според съдебния експерт дадените разпореждания от КЗЛД не касаят извършването на технически действия, като тези по т. 1, 2, 4, 9, 11, 12, 13, 14 и 15 касаят на практика процесите по анализ и идентифициране на потенциални заплахи, администрирането на лични данни, каквито не са изтекли при кибератаката. Специално за т.3 е посочено, че препоръчаните процедури съществуват и преди атаката. За т.5 и т. 7 от решението на КЗЛД съдебният експерт посочва наличието изпълнение на предписанието, по т.6 предвидени, но нереализирани политики за запис поради липса на финансови средства, а по т.16 е установило замяна на софтуера в рамките на месец след кибератаката. Направен е извод, че всички разпореждания са изпълнени.

При горните фактически установявания и във връзка със задължителните указания на ВАС в Решение №2633/14.03.2025г. по адм.д.№5991/2024г., настоящият съдебен състав формира следните правни изводи:

Чл.5, т.1, б.“е“ от Регламента, предвижда, че личните данни следва 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"); като съгласно т.2 администраторът носи отговорност и е в състояние да докаже спазването на параграф 1 („отчетност").

Съгласно чл.4, § 2 от Регламент 2016/679 „обработване" означава 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. Предвид това, съдът приема, че дори да

не се извлечени при кибератаката, като са криптирани съхраняваните от жалбоподателя личните данни, на същите е извършена обработка от трето неоторизирано лице чрез ограничаване на достъпа да тях по смисъла на чл.4, т.3 от Регламента, съгласно който „ограничаване на обработването" означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще.

Съгласно разпоредбата на чл.32, § 1 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, 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: псевдонимизация и криптиране на личните данни; 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.

Според § 2 на с.р. 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, а според § 4 администраторът и обработващият лични данни предприемат стъпки всяко физическо лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до лични данни, да обработва тези данни само по указание на администратора, освен ако от въпросното лице не се изисква да прави това по силата на правото на Съюза или правото на държава членка.

Чл. 24 от Общия регламент също въвежда като задължение и отговорност на администратора на лични данни да въведе подходящите технически и организационни мерки, отчитайки факторите, изброени в същия член.

Както отбелязва в задължителните си указния ВАС, чл. 24 и 32 от Общия регламент задължават администратора на лични данни (какъвто се явява „Български пощи“ ЕАД) да вземе подходящите технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с Регламента. Същите не са и не могат да бъдат конкретно посочени, защото подходът, който е възприет, е всеки администратор сам да определи кои да бъдат тези мерки. Съгласно „принципа за отчетност“, регламентиран в чл. 5, §. 2 от ОРЗД, той носи отговорност и следва да е в състояние във всеки момент да може да докаже спазване на принципите, закрепени в чл. 5, §. 1 от Регламента, при обработване личните данни на физически лица. Също така в гореспоменатите норми е предвидено, че тези мерки следва да бъдат преразглеждани редовно и при необходимост да се актуализират. В същия смисъл е и чл.59, ал.3 във вр. с ал.1 ЗЗЛД, за нарушение на който е предвидена имуществена санкция в чл.85, ал.4 ЗЗЛД.

В съображение 74 от Регламента е предвидено, че администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с настоящия регламент, включително ефективността на мерките.

Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица. В тежест на администратора на лични данни е да докаже, че е взел подходящите мерки за защита на личните данни, които обработва.

Също така, съгласно решение по дело С-340/21 г. на Съдът на Европейския съюз, членове 24 и 32 от 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“ по смисъла на тези членове 24 и 32. Следователно е основателен доводът на жалбоподателя, че законова презумпция няма.

Основният спор по делото е дали приложените от администратора към момента на издаване на оспореното решение технически и организационни мерки по чл. 32 от Регламента са подходящи с оглед рисковете, свързани със съответното обработване и дали естеството, обхватът и прилагането на тези мерки са съобразени с тези рискове. Администраторът на лични данни носи тежестта за доказване на обстоятелството, че приложените от него мерки за сигурност по чл. 32 от посочения регламент са подходящи, както и че те са били приложени към релевантния момент – издаването на решението.

От предоставените от „Български пощи“ ЕАД доказателства е установено предприемането на технически и организационни мерки от негова страна. За да обоснове, че тези мерки са били неподходящи и недостатъчни, КЗЛД се е мотивирала с кибератаката, при която са били криптирани съхранявани лични данни, като наложените в случая мерки са превантивни и целят да предотвратят занапред такива.

В тази връзка следва да се прецени, дали приложените от жалбоподателя технически и организационни мерки за защита на личните данни са били недостатъчни и неподходящи, поради което са станали необходима предпоставка за успешното реализиране на кибератаката. От заключението на вещото лице се установява, че това е станало поради деактивирането, по предписание на Microsoft, на важен модул, който защитава от спам и зловреден софтуер. Това действие на жалбоподателя, обосновава извода за извършено нарушение по Общия регламент относно защитата на данните, което е предпоставка по чл.22 ЗАНН във вр. с чл. 58, пар.2, б."г" от Регламента за налагане на принудителни административни мерки. За да прецени, обаче, дали тези мерси са целесъобразни, т.е. в съответствие с целта на закона, съдът съобрази следното:

Предписаните мерки по т.1, т.2, т.4, т.9, т.11, т.12, т.13, т.14 и т.15 от оспореното решение касаят процеси по анализ и идентифициране на потенциални заплахи (рискове), техническо изготвяне на критерии за сключване на договори с доставчици, сключване на такива, изготвяне на нови длъжностни характеристики на служителите на „Български пощи“ ЕАД и провеждане на контрол и обучение на служителите, т.е. касаят процеси по администрирането на лични данни от служители на жалбоподателя, неправомерно поведение на каквито не се установява в случая като причина за кибератката, която е осъществена от трети лица. Предвид това съдът приема горните принудителни мерки за неподходящи в случая. С тях на практика административният орган се намесва в оперативната самостоятелност на администратора на лични данни да организира процеса по обработката им, без да излага съображения как вече въведените правила са станали причина или са допуснали осъщественото неправомерно обработване.

Не са свързани с възможност за предотвратяване на кибератаки от вида на осъществената и предписанията по т.3, т.5, т.6, т.7 т.8, т.10 и т.16, още повече, че както сочи вещото лице такива мерки са предприети преди издаването на оспореното решение, а някой от тях /т.3, т.6, т.7, т.8/ и преди кибератаката.

Липсват конкретни предписания във връзка са установената по повод кибератаката уязвимост на системата, свързана с деактивирането на модул, който защитава от спам и зловреден софтуер.

Предвид гореизложеното съдът намира, че наложените в случая ПАМ не са необходими и подходящи, доколкото макар и да са наложени по повод осъществената кибератака, не са били в състояние да предотвратят същата, още повече, че част от тях вече са били приложени от жалбоподателя преди нея, а всички и преди издаването на оспореното решение.

По изложените доводи настоящият съдебен състав намира, че оспореното решение е незаконосъобразно и като такова следва да бъде отменено.

При този изход на делото, на жалбоподателят ще следва да се присъдят съдебни разноски за юрисконсултско възнаграждение в размер на 240лв.

Мотивиран така и на основание чл. 172, ал. 2 от АПК, Административен съд София-град, Второ отделение, 31 състав

Р Е Ш И:

ОТМЕНЯ Решение № ПАИКД-13-20/22 от 06.10.2022 г. на Комисията за защита на личните данни.

ОСЪЖДА Комисията за защита на личните данни да заплати на „Български пощи“ ЕАД, ЕИК[ЕИК], съдебни разноски в размер на 240 /двеста и четиридесет/ лева.

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

СЪДИЯ: