Р Е Ш Е Н И Е
№ 505

гр. София, 18.01.2024 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 33 състав,** в публично заседание на 30.11.2023 г. в следния състав:

СЪДИЯ: Галин Несторов

при участието на секретаря Антонина Бикова, като разгледа дело номер **9929** по описа за **2022** 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. 7, 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).

Образувано е 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.

Наведените основания за оспорване, предвид изложените в жалбата оплаквания и твърдения се квалифицират от съда по чл.146, т.3 и т.4 АПК-съществени нарушения на адиминистративнопроизводствените правила и противоречие с материалноправните норми-чл.146, т.3 и т.4 АПК. Твърди се, че дадените с оспореното административно решение разпореждания в т.1 до т.16 са много общо формулирани и непълно дефинирани, което създавало неясноти и препятствало тяхното изпълнение. Изразите „ясно разписани правила“, „да се предприемат подходящи технически и организационни мерки“, „пълен обем“, „достатъчно рестриктивни“, „прекомерни“ не били извлечени от конкретни разпоредби или стандарти и не били конкретизирани в самите разпореждания, поради което възпрепятствали възможността на жалбоподателя като администратор да изпълни разпорежданията в степен,

съответстваща на дадените формулировки. Недостатъчен бил и указаният срок за изпълнение по оспореното решение. Подържа се, че „Български пощи“ ЕАД е предприела всички необходими технически и организационни мерки за защита на данните за справяне с нарушението на сигурността на личните данни, което противоречи на констатациите на административния орган. Моли за отмяна на решението, алтернативно моли за удължаване на посочените в същото срокове за изпълнение.

В съдебно заседание жалбоподателят се представлява от юрк. Д., която поддържа жалбата на заявените основания и претендира юрисконсултско възнаграждение.

Ответникът – Комисията за защита на личните данни се представлява от юриск. Я., който моли за отхвърляне на жалбата.

Административен съд – София – град, след като обсъди доводите на страните и прецени по реда на чл. 168 ал. 1 АПК събраните и приети по делото писмени доказателства и законосъобразността на оспорвания административен акт като цяло, приема за установено от фактическа и правна страна следното:

Административното производство пред КЗЛД започва по повод уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679 (Регламента), с вх. № ПАИКД-13-20/18.04.2022 г. от „Български пощи" ЕАД. Образувана е преписка ПАИКД-13-20, по повод на което е извършена проверка на място и е събрана информация за случая.

Установено е както следва: на 16.04.2022 г. в 8:30 часа, при невъзможност за логване в информационните системи от касиерите за раздаване на великденски добавки на пенсионерите, е установена невъзможност за функциониране на софтуерните приложения в пощенските станции. Системните администратори разглеждат логовете на сървърите и установяват, че на S. клъстера, на който са базите данни, фигурира нерегламентиран администраторски акаунт и голяма част от базите са криптирани в резултат на хакерска атака. Засегнати са сървърни конфигурации на S. сървърите като са заразени с ransomware (злонамерен софтуер). Криптирани са файловете на базите данни, разположени на виртуалните машини, с разширение: T. decryption. Няма установени криптирани данни, разположени на физически отделни сървъри.

Извършена е оценка, в съответствие с "Инструкция за управление на инциденти, версия 02 от 26.09.2014 г.“: Значимост и въздействие: Приоритетен код 1 - „Критичен".

Незабавно е сформиран кризисен щаб с представители на службите за сигурност, всички доставчици на ИТ услуги и отговорните длъжностни лица. Активиран е „План за непрекъснатост на сигурността на информацията, версия 4/20.08.2018“, заедно с предвидените процедури за реакция при незаконна външна атака. На специалисти от ИТ компания „Telelink“ (W. и S. специалисти) е предоставен пълен достъп и съдействие в диагностиране на проблема и търсене на неговото решение.

Сформираните екипи за реакция работят върху всички аспекти на инцидента. Оценен е обхвата на въздействие върху активите и паралелно е това са извършени предвидените действия по възстановяването на IT инфраструктурата и основните платформи за възобновяване на услугите.

В 72-часовия период след узнаване за нарушението са предприети следните действия от страна на Администратора:

- 8:24 ч. на 16 април 2022 г. - първите уведомления до системните администратори и мрежовия администратор за невъзможност да се свържат с касов

модул (S. сървър);

- 8:30 ч. на 16 април 2022 г. - за проблема е докладвано на директора на Дирекция „Информационни и комуникационни технологии“ („ИКТ“), който сформира екип за реакция;
- 8:45 ч. на 16 април 2022 г. — мрежовият администратор установява, чрез софтуера за наблюдение, S. сървър чиито процесори работят на 100%, като уведомява администратора на базите данни и директора на дирекция „ИКТ“;
- 9:10 ч. на 16 април 2022 г. към директора на дирекция „ИКТ” постъпват уведомления от администраторите за неработещи системи

. • 9:15 ч. на 16 април 2022 г. - директорът на дирекция „ИКТ" нарежда проверка на всички администратори на системи;

- 9:17 ч. на 16 април 2022 г. - уведомен е главния изпълнителен директор, с оглед уведомяване на висшето ръководство;
- 9:30 ч. на 16 април 2022 г. - осъществена е комуникация с представители на отдел „Киберпрестъпноет“ към Главна дирекция ..Борба с организираната престъпност" (ГДБОГ1);
- 10:47 ч. на 16 април 2022 г. - директорът на .дирекция ..ИКТ" нарежда на администратора на отдел „Административна дейност" проверка и спиране на международния интернет;
- На 16 април 2022 г. е осъществена комуникация със служител на дирекция „Информационна сигурност" към Държавната агенция ..Национална сигурност" (ДАНС);
- На 16 април 2022 г. е осъществена комуникация с директора дирекция „Информационна сигурност“ към ДАНС;
- Уведомен с Центъра за действие при инциденти в информационната сигурност (CERT);
- 12:08 ч. на 16 април 2022 г. - уведомен е доставчика па антивирусния софтуер Kset NOD 32 за сформиране на екип и експертна помощ;
- 12:10 ч. на 16 април 2022 г. - уведомен е доставчика на защитните стени eFellows за сформиране на екип и експертна помощ;
- 12:17 ч. на 16 април 2022 г. - мрежовият администратор създава правило на вътрешната двойка защитни стени Р. А., с което спира международния интернет, предоставяйки възможност на администратора на базата данни, администратора на отдел „Административна дейност“, екипите па eFellows, отдел „Киберпрестъпноет" към ГДБОП и ДАНС да имат отдалечен достъп през V. за проверка и анализ на бекъпите;
- 12:40 ч. на 16 април 2022 г. - министърът на електронното управление се обажда на директора на дирекция „.ИКТ" и се информира за обстановката;
- 13:20 ч. на 16 април 2022 г. - кризисният щаб преминава в присъствен режим и се създава ситуационен център в зала 212 на Централно управление (ЦУ) на Български пощи;

От 13.26ч до 14.00ч на 16 април 2022г. в ситуационният център пристигат последователно екипите на ДАНС, eFellows, отдел „Киберпрсстъпност“ към ГД Б. и продължават дейностите присъствено. В екипа са включени експерти от Министерството на електронното управление (МГУ), основните доставчици - „Виваком“; екип по киберсигурност на „Телелинк";

• 21.22 ч. на 17 април 2022 г. eFellows създават правило на Р. А., е което спират

интернета на сървърите изцяло.
В резултат от предприетите действия е констатирано компрометиране на информационната инфраструктура на Администратора, спиране на основни услуги, нарушаване на целостта и поверителността на информацията вследствие на допускане и липса на обезвреждане на злонамерен софтуер в компютърната мрежа.
Чрез доклад до началника на кабинета на заместник – министър-председателя по ефективно управление принципалът на дружеството е уведомен относно качествената и количествената оценка за претърпените щети, анализа па причините довели до атаката и предприетите мерки за повишаване защитата на инфраструктурата.
Изпратено с уведомление за инцидента до Националната агенция за приходите (НАП).
Предприети са действия за служебно дерегистриране на всички обекти от Интегрирана автоматизирана система за управление на търговската дейност (ИАСУТД) с цел недопускане и предотвратяване на евентуален пробив на междуведомствените системи и НАП.
Съвместно с експертите от НАП е обсъдено и по тяхно настояване е извършено деактивирано на всички виртуални карти (3050 бр.), осигуряващи онлайн отразяване на транзакциите в системата па агенцията.
Направен е извод, че външните нападатели не са имали непосредствен физически контакт с информационната система на Български пощи, което предполага използване на някакъв вид агенти за проникване в нея преди извършване на вредителските действия. В такова качество може да се използва връзката с глобалната мрежа и нейните услуги, поведението на служители на организацията, разпространението па вредителски код и т.и.
Това, което е установено след обстоен одит на информационната инфраструктура е пробив на сигурността на информационната инфраструктура посредством зловреден софтуер Mimikatz: платформа за кражба на пароли. Инструментът Mimikalz е 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 W..
Използвана е уязвимост в сигурността на M. пощенски сървър, чрез която нападателите придобиват достъп до вътрешната памет на W. системите. Оставен е лог със следната информация:
„U. for you, a major IT security weakness left you open to attack, your files have been encrypted.
If you want to restore them, write to our skype - T. Decryption
Also you can write ICO live chat which works 24/7 @Thomasdecryption
I. ICO software on your PC https://icq.com/windows/ or on your mobile phone search in Appstore / G. market I.
W. to our ICO (afThomasdecryption https://icq.im/Thomasdecryption
If we not reply in 6 hours you can write to our mail but use it only ifprevious methods not working - [електронна поща]
Бяха ИЗТЕГЛЕНИ чувствителни данни във вашата система.
Ако НЕ ИСКАТЕ вашите чувствителни данни да бъдат ПУБЛИКУВАНИ, трябва да действате бързо.“
Зловредният софтуер блокира потребителите от използване на собствените им информационни системи и криптира файлове и бази данни, като дава на нападателите контрол пад всяка информация, съхранявана на сървърите на Администратора.

Екипът от експерти е извършил пълна инспекция па всички сървъри и работни станции. След диагностиката е установено, че бекъпите на базите данни също са криптирани, което допълнително усложнява ситуацията.
По време на работата на екипите за реакция на 19 април 2022 г. в 23:17 ч. е констатирана последваща атака ICMP F. към външния DNS, която претоварва защитната степа и се налага спиране на интернет достъпа.
На 20 април 2022 г в 09:40 ч. отново е активирана страницата на Български пощи и в кратък срок, около 20 минути, атаката е подновена.
От предоставената по време на проверката документация, от извършения мониторинг на трафика през защитните стени, за периода 1-16 април 2022 г., не е установен завишен трафик, различен от нормалния, което води до извода, че данните не са изтеглени от информационната система (няма разпространение на неправомерно достъпените данни). На електронен носител са приложени наличните логове за 2022 г. до 16 април 2022 г.
С оглед на събраните по преписката доказателства, комисията за защита па личните данни е констатирала, че действително е възникнало събитие, представляващо случай на нарушение на сигурността на личните данни по смисъла на чл. 33 от Регламент (ЕС) 2016/679.
На основание анализ на представените документи и осъществената проверка на място е установено, следното:
1. Администраторът не е успял да приложи подходящи технически и организационни мерки, поради което, в резултат на неоторизиран достъп, са криптирани бази данни с приблизително 4 675 393 бр. записи, съдържащи лични данни на физически лица, от които индивидуализирани са 675 393 бр. физически лица. Вследствие на това е нарушена 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 личните данни.
2. В резултат на хакерската атака е осъществен нерегламентиран достъп до информационните системи и приложения. От извършения мониторинг на трафика е установено, че през защитните стени, за периода 1 април 2022 г. - 16 април 2022 г., не е установен завишен трафик, т. е. не са събрани данни за разпространение на достъпената информация.
3. Липсват политики и процедури за формиране и поддръжка на журнални дневници (лог файлове).
4. Не са спазени процедурите и политиките за архивиране (бекъп) на информационните системи. Нс 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. В резултат на това Български пощи е в невъзможност да възстанови функционирането на информационните системи и бази данни. Възстановени са единствено информационната система ИКИС от направен бекьп предишния ден и информационната система Е., която с възстановена от файл за изплащане на следващите пенсии, подучен от НОИ след инцидента.
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

DB администратора - user name: Amelikian, password: 96101404k, са недостатъчно надеждни, неотговарящи на изискванията за информационна сигурност (слаба администраторска парола), като потребителското име включва името на А. М. (ръководител на отдел „Бази данни"). Съгласно утвърдена в Български пощи практика, потребителските имена на служителите за достъп до информационните системи и ресурси са техните имена:

6. Извършения годишен одит на информационната система по стандарт ISO 27001:2013 касае единствено информационната сигурност. Няма изградена система за проверка на защитата на личните данни и стандартът не е надграден до ISO/IEC 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, пар. 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. 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.

8. Не са събрани доказателства, че утвърдените от Български пощи политики и процедури са приложени в цялост на практика в дейността на Администратора.

9. Липса на последващ контрол, за усвоеното от служителите, след приключване на обучението по Регламент (КС) 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 характеристиките включени клаузи, касаещи обработването на лични данни.

11. При извършения вътрешен одит през 2021 г. по 1S0/IEC 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 външна намеса и прекъсване на услуги, вследствие отказ па комуникационни устройства ". Не са предприети бързи и адекватни мерки за защита по отношение констатираните 2021 г. уязвимост, водещи до увеличаване на рисковете, а дирекция „ИКТ" е планирала в инвестиционната програма пет инвестиционни проекта със срок за изпълнение 2021 г. - 2023 г. за преодоляване на високите нива на риск.

12. Нарушен е принципът на отчетност - липсват одитни записи на отделните събития и журнал ни дневници за привилегированите потребители. Няма внедрена система за тяхното управление (Privileged Access M.. 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 (SIEM) за оешурнване 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 „Защита на личните данни". Основните отговорности за работоспособността на информационните системи

са съсредоточени в дирекцията „ИКТ“.

15. Но време па проверката не са събрани доказателства за реализация на P. By D., P. By Redesign и P. By Default, изразяващо се в провеждане на консултации с длъжностното лице но защита на личните данни по отношение разработване или закупуване на информационна система и оборудване. Не се осъществяват периодични консулт ации с него, с оглед анализа на техническите и организационните мерки за зашита 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 такива с изразено негово експертно мнение

16. Липсват доказателства за периодична ангажираност на висшия мениджмънт за запознаване е проблемите на информационната сигурност и нейното ресурсно осигуряване.

17. Нс са предприети действия за обновяване на операционните системи и на СУЬД към актуални версии на M. S. (версия S. 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 администратор-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 е видно, че 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.

При горните установявания КЗЛД е приела, че от страна на администратора на лични данни „Български пощи“ ЕАД не са приложени подходящи технически и организационни мерки, в резултат на което е извършен неоторизиран достъп до негови бази данни, след което същите са били криптирани. От нарушението на сигурността са засегнати приблизително 4 675 393 бр. записи, съдържащи лични данни на физически лица, 1 700 000 субекти на данни от Интегрираната автоматизирана система за управление на търговската дейност (ИАСТУД), от които индивидуализирани са 675 393 бр. физически лица. В резултат на това е нарушена способността за гарантиране па постоянна поверителност, наличност, цялостност и устойчивост на системите и услугите за обработване, както и способността за своевременно възстановяване па наличността и достъпа до личните данни, с което с нарушен чл. 32, § 1, б. „б“, „в“ и „г“ и § 2, във връзка с чл. 5, § 1,6. „е“ от Регламент (ЕС) 2016/679.

С оглед установеното в резултат на извършената проверка КЗЛД прецени като най-целесъобразно да приложи мярката но чл. 58, пар. 2, б. „г“ от Регламент (ЕС) 2016/679, а именно да даде конкретни разпореждания на Администратора, включително, като му укаже и начина, по който следва да отстрани

констатираните нарушения.
Така с оспореното административно 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 журнал пи записи (догове). 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 M., PAM) и Система за управление и анализ на събитията, отразени в дневниците (S. 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 па 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 но 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 (т ри) месеца от влизане в сила на решението;

13. Да въведе и приложи механизми за последващ контрол на ефективността на проведените обучения на служителите но защита на линиите 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 па системите за управление па 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;
За изясняване на релевантните за делото обстоятелства е изслушана и приета съдебна компютърна техническа експертиза (СКТЕ), която съдът кредитира изцяло. Според заключението на в.л. инж. Д. С. пробивът в сигурността в „Български пощи“ ЕАД е настъпил на 15.04.2022 в 22:20 до 22:21ч.- нощта на петък срещу събота. Разкритието на инцидента се е случило на 16.04.2022г. в 08:24 ч. в момент, в който все още хакерът не е успял да архивира и подготви напълно данните и да започне да изтегляне. Логове от сървърите не са запазени към момента на експертизата. Към момента на атаката Български пощи е използвал множество видове софтуер, като един от тях е E. Server 2016 на M.. Екипът по информационна сигурност на “Български пощи” ЕАД води (и към датата на атаката също) регистър на инциденти.
Според вещото лице в конкретният случай не се касае за извличане на информация. Касае се за изтриване/промяна/криптиране на информация, както и за изваждане на системите от експлоатация. В конкретният случай нерегламентираният достъп е бил осъществен през E. Server 2016. P. на софтуер, в случая M. прави регулярни ъпдейти на системата с цел да “запуши” слабите места на системата. На разработчикът е бил известен проблем със сигурността на E. Server 2016 и E. Server 2019. Временното решение на M. включва спиране на FIP-FS скенера, което увеличава рисковете от спам и потенциално зловреден софтуер. Към месец август 2022 г. проблемът все още не е решен от M..
Според регистъра на инциденти последователността на действията на нерегламентираният достъп са както следва:
- Пробивът е осъществен, като зловредните файлове са били създадени/ копирани на хост S.-OFFLINE-APP НА 15.04.2022 от 22:20 ч. до 22:21ч.;
-след което в 22:28 ч. е направена успешна RDP сесия (отдалечена сесия на протокола за отдалечен работен плот R. Desktop) на BGPOST-EXCH16-1 от установен IP адрес с потребител „administrator“
-в 22:31 ч. на BGPOST-EXCH16-1 е създадена папка „mimi“, където са качени/копирани инструментите зловреден софтуер с платформата за копиране на пароли;
-от 23:17 ч. на 15.04.2022 до 07.52 ч. на 16.04.2022 последователно на S. (базата

данни);
Според СКТЕ единствената причина за нерегламентираният достъп до системата е деактивирането, по предписание на производителя М., на важен модул, който защитава от спам и злонамерен софтуер. При липса на тази уязвимост в М. Е., такъв вид нерегламентирано проникване е невъзможно.
Вещото лице дава заключение, че препоръките на КЗЛД представляват 16 точки, по-голямата част от които не касаят технически действия. Точки 1, 2, 4, 9, 11, 12,13, 14, 15, касаят процеси по администриране на лични данни, каквито не са изтекли при кибератаката от 16.04.2022 г.
Точка 3 касае актуализация на процедурата по формиране на потребителски имена и пароли и да внедри приложения за предпазване от разкриване на пароли.
Такава процедура има в дружеството и преди атаката, като пробивът не е станал в следствие на brute force атака. B. force атаката се използва за опити за откриване на потребителски пароли чрез пробване на множество комбинации от символи. Атакуващият не използва специфични уязвимости, а просто изпробва всички възможни комбинации, докато не намери правилната парола.
Пробивът е осъществен, като зловредните файлове са били създадени/копирани на хост S.-OFFLINE-APP.
Точка 5. Преди инцидента е съществувал регистър на инцидентите, на базата на който са направени и анализите след това.
След инцидента на всички сървъри в новата среда е инсталирана ефективна XDR система. Анализът и мониторингът откриват активност, поведенчески модели и други предупредителни знаци, които традиционните техники за сигурност биха пропуснали. П. е изпълнено.
Точка 6. Преди инцидента е била въведена политика по запис и поддръжка на лог файлове. SIEM и DLP системи са били заложени в бизнес плана на Български пощи ЕАД, но поради липса на финансови средства не са били реализирани. Предвидено е внедряване на система за управление на нива на достъп до корпоративните платформи и приложения - Privileged Access M. (PAM).
Предвидено е също така изграждане на комплексно решение за отдалечен непрекъснат мониторинг на сигурността, наричано Система за мониторинг, анализ и контрол на логове, мрежови трафик, системни файлове и управление на кибер-инциденти от служители на изпълнителя, за нуждите на Български Пощи ЕАД.
Точка 7. Към датата на инцидента бекъп файлове са били създавани и съхранявани съобразно тогава действащите вътрешни правила на “Български пощи” ЕАД. След инцидента инфраструктурата на дружеството и към датата на експертизата се намира в ДХЧО (Държавен хибриден частен облак) и съхранението на архивни копия е свързана с услуга „Виртуален център за данни“ и управлението и съхранението на резервните копия, създавани от услуга V. M. Backup as a S.. Разработена е стратегия за резервен център и пълен

архив на базите П. е изпълнено.
Точка 8 е изпълнена преди инцидента.
Точка 16. Замяната на софтуер се извършва непрекъснато в Български пощи ЕАД, в зависимост от предварително разписани цели.
След инцидента в рамките на 1 един месец, всички машини, които са използвали W. 7 са били транспортирани до централния офис на дружеството и са били преинсталирани с по-нова актуална към момента версия.
Дадените препоръки касаят основно защита и съхранение на лични данни, но не касаят предотвратяне на бъдещи атаки.
В заключение СКТЕ сочи, че всички препоръки вече са били изпълнени от "Български пощи" ЕАД, когато са предписани.
При горните фактически установявания съдът формира следните правни изводи:
Жалбата е процесуално допустима за разглеждане. Решението на КЗЛД е получено на 10.10.2022 г., а жалбата е депозирана на 24.10.2022 г. Жалбата е подадена от надлежна страна - адресат на акта, за която е налице и пряк и непосредствен интерес от обжалването на засягащите я предписания.
Разгледана по същество жалбата е неоснователна.
Оспореното решение е издадено от компетентен орган- КЗЛД. Съгласно чл. 6, ал. 1 ЗЗЛД, КЗЛД е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на този закон и на Регламент (ЕС) 2016/679. Правомощието на КЗЛД за извършване на проверки е регламентирано изрично в чл. 12 от ЗЗЛД, съгласно която норма - Председателят и членовете на комисията или упълномощени лица от администрацията й, осъществяват контрол чрез проверки за спазване на Регламент /ЕС/ 2016/679. В този смисъл оспореното решение е постановено от компетентен орган.
Обжалваното решение е прието е при необходимия кворум и с необходимото мнозинство - арг. чл. 9, ал. 3 от ЗЗЛД и чл. 8, ал. 6 и ал. 7 от Правилника. Съгласно чл. 7, ал. 1 от ЗЗЛД комисията е колегиален орган и се състои от председател и 4 членове, а решенията се вземат с мнозинство от общия брой на членовете (чл. 9, ал. 3). Същото следва да бъде подписано от всички членове, участвали в гласуването. В случая за оспореното решение са гласували четирима със "за" и нито един против, поради което безспорно е формирано мнозинство и решението е валидно взето. В тази връзка не е осъществено основанието по чл. 146, т. 1 АПК.
Спазена е установената от закона форма - актът е в писмена форма, посочени са фактическите и правни основания за издаването му. Същият съдържа изискуемите от разпоредбата на чл. 59, ал. 2 АПК реквизити, доколкото приложимият специален закон - ЗЗЛД не съдържа специални изисквания към формата и съдържанието на акта. Оспореният акт съдържа ясна разпоредителна част, посочени са релевантните факти и обстоятелства и приложимите според

административния орган правни норми, проявлението на които обосновава разпоредените от него правни последици.
В хода на административното производство не са допуснати съществени нарушения на административнопроизводствените правила, които да водят до отмяна на оспорения акт. Във връзка с подадено уведомление от „Български пощи“ ЕАД е разпоредено извършване на проверка по спазване и прилагане на Регламент (ЕС) 2016/679 и на ЗЗЛД; събрани са доказателства; предоставена е възможност на жалбоподателя да представи доказателства; изготвен е констативен акт от проверяващ екип; събраните доказателства са обсъдени на заседание на КЗЛД, на което с единодушие е взето решение.
По правилното приложение на материалният закон съдът съобрази следното:
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 е 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.
Следва да се отбележи, че 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. Това задължение не може да бъде дерогирано от осъществяването

на специфична административна дейност от администратора. 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.

Жалбоподателят излага твърдения, че КЗЛД неправилно е приела, че техническите и организационни мерки, предприети от него, не са били достатъчни. От извършения анализ на предоставените от „Български пощи“ ЕАД доказателства е установено, вземането на технически и организационни мерки от негова страна, но липсват доказателства, от които да се направи обоснован извод, че са подходящи, за да гарантират защита на данните. Не е доказано, че предприетите технически и организационни мерки, са били в такава степен подходящи и ефективни, че да гарантират обработването на личните данни в съответствие с изискванията на Регламент (ЕС) 2016/679. 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 налични данни е да докаже, че е взел подходящите мерки за защита на личните данни, които обработва. Неправомерното поведение на трети лица, извън служителите на жалбоподателя, не се съвместява с правилата, които следва да бъдат въведени и по възможност гарантирано спазвани от администратора на лични данни.

Комисията разполага с оперативна самостоятелност като в съответствие с предоставените ѝ функции преценява кое от корективните правомощия по чл. 58, § 2 от Регламент (ЕС) 2016/679 да упражни. Преценката следва да се основава на съображенията за целесъобразност и ефективност на решението при отчитане особеностите на всеки отделен случай и степента на засягане на интересите на конкретното физическо лице – субект на данни, както и на обществения интерес. Правомощията по чл. 58, § 2 от Регламент (ЕС) 2016/679, без това по б. „и“, имат характера на принудителни административни мерки (ПАМ), чиято цел е да предотвратят или да преустановят извършването на нарушение, като по този начин се постигне целеното поведение в областта на защитата на личните данни. Изцяло от преценката на надзорния орган зависи дали да приложи спрямо конкретния случай някоя от ПАМ, регламентирани в б. „а“ – „з“ и „й“ или да наложи административно наказание „глоба“ или „имуществена санкция“ или да приложи и някоя от мерките съвместно с

административно наказание по б. „и“. При определяне на корективната мярка следва да бъде съобразена целта, която се преследва с налагането й и дали с изпълнението й тази цел ще бъде постигната.
В процесният случай, в условията на предоставената й оперативна самостоятелност, КЗЛД е приела да приложи корективната мярка по чл. 58, § 2, б. „г“ от Регламент /ЕС/ 2016/679.
По същество се касае за 16 мерки, описани по-горе в изложението, които според приетата по делото съдебно компютърна техническа експертиза, в частта, свързана с компютърната сигурност (разпореждания по т. 3, 5, 6, 7, 8, 10 и 16) вече са изпълнени. Последното, доколкото е съдебно установено, следва да бъде взето предвид и от административният орган с оглед разпореждането за предоставяне на доказателства за изпълнение на разпорежданията.
Разпореждания по точки 1, 2, 4, 9, 11, 12, 13, 14, 15, 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.
Според съдът така описаните разпореждания се определят като съответни на материалният закон, доколкото по-голямата част от тях вече са били изпълнени, а останалите, за които няма данни по делото да са изпълнени имат чисто технически характер. Така в случая се касае за актуализиране на длъжностни характеристики, договори и провеждане на обучение, чиито срокове са между 3 и 6 месеца от влизане в сила на решението на КЗЛД, който срокове съдът счита за уместни. Касателно идентификацията и анализ на рисковете по мнение на съда това се извършва по повод и във връзка с обработването на лични данни, независимо от това, как са станали достояние на администратора и дали те са от публични регистри или не, и се извършва постоянно по арг. от чл. 32, § 1, б. „г“ от Регламента.
В конкретния случай нарушението не възниква само вследствие на субективен източник на риск - поведението на служител, а и поради недостатъчност на въведените технически и организационни мерки за защита на сигурността на данните в „Български пощи“ ЕАД. Оценката на риска е условие за съответствие с Регламент (ЕС) 2016/679 и по принцип, администраторът следва да извършва периодични такива, за да може да го постигне. Тя е от съществено значение за ефективността на мерките за сигурност, въведени от него, както и средство, чрез което той може да идентифицира потенциален проблем, който в бъдеще да причини материални или нематериални вреди.
С прилагането на Регламент (ЕС) 2016/679, за администраторите на лични данни възниква задължението за извършване оценка на риска на дейностите по обработване на лични данни и въвеждане на подходящо ниво на сигурност. Неизвършването на такава означава, че след като не са могли да бъдат идентифицирани потенциалните рискови фактори, не е могло да бъдат предприети подходящи технически и организационни мерки, за да се гарантира

подходящо ниво на сигурност на обработването, което да осигури постоянна поверителност, цялостност, наличност и устойчивост на обработваните от администратора лични данни, както и на системите за обработване на личните данни. Следва да се отбележи, че чл. 24 от Общия регламент въвежда като задължение и отговорност на администратора на лични данни да въведе подходящите технически и организационни мерки, отчитайки факторите, изброени в същия член.

Налага се извода, че законосъобразно и мотивирано е упражненото от страна на Комисията корективно правомощие по чл. 58, § 2, б. „г“ от Регламент 2016/679, а именно: КЗЛД е разпоредила на администратора на лични данни да изпълни определени разпореждания (част от които съдебно са установени, че са изпълнени), като след изтичане на указания срок да уведоми КЗЛД за изпълнението, като представи съответни доказателства.

По изложените доводи настоящият съдебен състав намира, оспореното решение е законосъобразно и като такова не подлежи на отмяна.

При този изход на делото на ответника се следват разноски, но такива не са претендирани, поради което не се присъждат.

Мотивиран така и на основание чл. 172, ал. 2 от АПК Административен съд София – град, II о., 33-ти състав

Р Е Ш И:

ОТХВЪРЛЯ 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.

Решението подлежи на обжалване чрез Административен съд София-град пред Върховен административен съд на РБ в 14-дневен срок от съобщаването му на страните.

Решението да се съобщи на страните чрез изпращане на препис от него по реда на чл.137 от АПК.

СЪДИЯ: