Р Е Ш Е Н И Е
№ 7990

гр. София, 26.02.2026 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 37 състав,** в публично заседание на 16.12.2025 г. в следния състав:

СЪДИЯ: Адриан Янев

при участието на секретаря Кристина Алексиева, като разгледа дело номер **2360** по описа за **2025** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145 – чл. 178 от Административнопроцесуалния кодекс (АПК) във връзка с чл. 38, ал. 8 от Закона за защита на личните данни (ЗЗЛД).

Образувано е по жалба на „Стеник груп“ ООД срещу Решение № ПАИКД-13-33/2024 на Комисията за защита на личните данни.

В жалбата са изложени съображения, че органът погрешно е квалифицирал жалбоподателя като администратор на лични данни. В подкрепа на това се посочва, че жалбоподателят не определя целите и средствата за обработка на лични данни, а само изгражда функционалности и осигуряване на функционирането на електронния магазин. Същият обработва лични данни само във връзка с предоставянето на услуги по поддръжка на свои клиенти – електронни магазини, които определят целите и средствата на лични данни. Оспорва констатациите на органа за осъществен нерегламентиран достъп чрез административен панел на жалбоподателя за достъп до електронните магазини. Поддържа се, че не разполага с такъв панел, а последният е на разположение на клиентите (собственици на електронни магазини). Допълните се поддържа за липсата на доказателства за осъществен нерегламентиран достъп до лични данни и за реално осъществено нарушение на сигурността на данните. Единствената индикация за това е писмо от анонимно лице, но няма доказателства за действително извършен достъп до лични данни. Също така липсвало разгласяване на предполагаемо изтеклите лични данни. КЗЛД не е извършила действия за проверка дали е осъществен достъп, до какви лични данни, за какъв брой лица, за кои администратори на лични данни и какви мерки за сигурност са преодолени. Не била съобразена дадената препоръка за въвеждане на двуфакторна автентикация, което е извършено преди твърдяното нарушение, а жалбоподателят не може по своя инициатива да въведе такава мярка за

сигурност. Даването на такава препоръка на собствениците на електронни магазини не било задължение на жалбоподателя, а само израз на загриженост и допълнителни усилия. От жалбоподателя били въведени процедури за защита на лични данни (съставяне на вътрешна инструкция и провеждани периодични срещи на GDPR бордове).
Ответната страна - Комисията за защита на личните данни, чрез процесуалния си представител, е подала отговор на жалбата, с който изразява становище за нейната неоснователност.
След като обсъди релевираните с жалбата основания, прецени становищата на страните и събраните по делото доказателства, съдът намира за установено следното от фактическа страна:
По преписката е приложен имейл от 02.03.2024 г. (л. 255 гръб и л. 485 гръб), озаглавен „Компрометирана пощенска кутия (stenik.bg), който е изпратен от отдел „Сигурност“ на жалбоподателя до друг негов отдел („продажби“). Уведомява се за извършена промяна на парола на пощенски кутии на хостинг акаунта за stenik.bg – [електронна поща] и [електронна поща] Посочено е, че спамъри са използвали пощенската кутия, за да изпращат спам на други потребители. Дадена е препоръка за сканирани на устройствата, използвани за достъп на пощенските кутии, за вируси и зловредни програми, както и за използване на криптирана връзка и сложни пароли.
По преписката е приложен имейл от 20.03.2024 г., изпратен от лице, представящо се като „K. D.“, адресиран до жалбоподателя „Стеник груп“ ООД (наричан още за краткост „Стеник“). В същия се твърди, че в периода от 03.03.2024 г. до 05.03.2024 г. е успял да източи съхранявани лични данни от 40 клиенти на жалбоподателя, отнасящи се приблизително 2 000 000 души, включващи имена, адреси, телефонни номера и имейли. Посочено е, че се прилага скриийншотове от източени лични данни. Като доказателство за пробива се предоставя датабазата на Айко, съдържаща данни на около 60 000 души и над 141 000 поръчки (посочен е конкретен линк), както и output от съдържанието на папката, в която се съхраняват данните. Поискан е откуп в размер на 65 000 лева, платим в Bitcoin. Данни за контакт е посочен потребител в Т.: .
По преписката е приложен имейл от 22.03.2024 г., изпратен от лице, представящо се като „samokovetsa“, адресиран до няколко имейли на жалбоподателя „Стеник груп“ ООД (наричан още за краткост „Стеник“). Посочва се, че същият е изпратен по повод липсата на отговор по първия имейл. Твърди се, че жалбоподателят не е свалил приложената датабазата на Айко, за което пояснява, че се представя датабазата на 8hristo.com. Твърди се, че притежава датабазата на Хиполенд, съдържаща лични данни на над един милион души. В края на имейла се сочи за предоставени 111 директории и 2713 файла.
Приложен е имейл от 28.03.2024 г., изпратен от лице, представящо се като „samokovetsa“ и „K. D.“, с който се настоява за плащане на сумата.
На 10.04.2024 г. е изпратен имейл от „samokovetsa“ до няколко имейли на жалбоподателя „Стеник груп“ ООД, който е със следното съдържание „20 000 или лично ще се свържа с В.“. Като заглавие на имейла е посочено датабаза на и са приложени снимки.
С имейл от 31.03.2024 г., изпратен от „K. D.“, се уведомява жалбоподателят, че е видял отварянето на скрийншотовете.
Приложен е сигнал на жалбоподателя, адресиран до ГДБОП, който е по повод изпратените имейли. Към сигнала са приложени обяснения от представителя на жалбоподателя, в които е отразена възможността за осъществен достъп до личните данни на клиентите на електронни магазини. Посочено е, че сървърът, на който функционират електронните магазини, се обслужва от Стеник по възлагане на клиенти, до който не е осъществен достъп. Предполага се, че пробивът и достъпът до лични данни е осъществен през административния панел на Магенто – логин с потребителско име и парола. Предполага се за осъществен неправомерен достъп до компютър на

някой от служителите на Стеник и по тази начин хакерът се сдобил с различни пароли, които ги е използвал при атаката. С категоричност не може да се посочи за осъществен неправомерен достъп до личните данни, а само е изложено предположение за такова и за техния вид (имена, телефон, имейл, адрес и ЕГН на клиенти на електронни магазини, които се поддържат от Стеник). Не може да се установи броя на засегнатите лица, тъй като хакерът не е оставил следи от експортиране в административния панел на онлайн магазините. Изчакано е да измине период преди да се извърши уведомяване, през което логовете на сървъра са изтрити, тъй като се съхраняват 2 седмици. В изпратения от хакера output файл се виждал достъп до сайтовете и имена на експорти, които са правени, като е представен семпъл на база данни на един клиент.

С уведомление от 01.04.2024 г. (л. 90 – л. 93) на жалбоподателя се дава информация на КЗЛД по нейно искане. Посочва се за извършена вътрешна проверка след получаване на анонимния имейл от 20.03.2024 г., на която е констатирано, че неправомерният достъп е осъществен през административния панел на електронните магазини, обслужвани от жалбоподателя. Посочва се, че хакери са разбили фирмения G. Password Manager на Стеник (съдържащ към онзи момент пароли за клиентски административни панели), посредством хакване на компютър на служител. Осъществен е достъп до административните панели с потребителски имена и пароли, ползвани от Стеник. Нерегламентираният достъп е осъществен през акаунта на жалбоподателя с username stenik (логин в административния панел). Този достъп е било възможно да бъде направен и от друго устройство, поради липсата на двуфакторна автентикация, която не е направена поради нежелание на клиентите да я активират. Историята за извършените действия била видна само 7 дни назад, при което е извършено връщане на back-up на системата. Установено е извършен експорт на данни клиенти и поръчки, които включват имена, имейл, телефонен номер и адрес. В тази връзка се посочва за наличието на нотификация за генерирани експорти, които вероятно били изтрити. Към уведомлението е приложен списък на собствениците на електронни магазини (26 бр.), обслужвани от жалбоподателя, в който е отразен максималният брой потенциално засегнати физически лица – клиенти на съответния електронен магазин. Посочва се, че отношенията с клиентите на жалбоподателя са регламентирани с договор за поддръжка и отделено споразумение за управление на лични данни. Уточнява се, че собствениците на онлайн магазини имат администраторски достъп с акаунти, който е различен за всеки проект, но при всеки от тях „Стеник груп“ ООД има 1 активен администраторски акаунт, с който се осъществява достъп до административния панел (втори се създава при конкретна нужда и се изтрива след отпадането ѝ). Посочва се, че не са налице доказателства за извличане на лични данни, а единствено косвени индикации за такова извличане.

Издадена е Заповед № РД-15-449/21.10.2024 г. на председателя на КЗЛД, с която е наредено да се извърши проверка на „Стеник груп“ ООД за спазване на Регламент (ЕС) 2016/679.

С уведомление на КЗЛД (л. 159 – л. 162 и л. 374 гръб) жалбоподателят е уведомен, че на 23.10.2024 г. ще се извърши проверка и е предоставен въпросник.

С молба от 22.10.2024 г. (л. 163169 и л. 376) на жалбоподателя е отговорено на изпратения въпросник.

Представен е доклад за извършена оценка на риска на сигурността и защитата на лични данни в сървъра с данни на клиенти на електронни магазини, поддържани от „Стеник груп“ ООД (л. 170 – л.171). В същия е отразено получаването на имейла от анонимно лице, в който се твърди за осъществен неправомерен достъп до лични данни. След извършена проверка е направен извод, че е възможно да осъществен такъв достъп или да са извлечени лични данни на клиенти на електронни магазини (име, имейл, ЕГН, телефонен номер, адрес и данни за артикули от съответните поръчки). Посочено е, че не е бил обект на хакерска атака сървърът, на който

функционират електронните магазини, обслужвани от Стеник. Според доклада пробивът и достъпът до лични данни е осъществен през административния панел.
Приложен е Констативен протокол от 23.10.2024 г. (л. 426), съставен по повод извършена проверка на жалбоподателя. Отразено е извършено демонстративно осъществяване на достъп до платформата Магенто и достъп до определени магазини на сървърно ниво.
По преписката е представен документ със заглавие „Среща КЗЛД и Stenik 23.10.2024“ (л. 481), който е заверен „вярно с оригинала“ от представител на жалбоподателя, за което е положен подпис. Посочено е, че на 05.03.2024 г. е установен извършен нерегламентиран достъп до уеб сайта на Stenik и два фирмени имейл адреса, които са използвани за разпращане на спам. На същата са взети незабавни мерки за повишаване на сигурността, за което са изпратени имейли до всички клиенти на жалбоподателя с препоръки за смяна на паролите и напомняне за активирани на двуфакторна автентикация като допълнително средство за защита на административния панел на електронния магазин (втората препоръка била повторна, тъй като на 25.08.2023 г. била вече дадена). Отразено е, че двата имейл адреси не се ползват за достъп до административния панел на онлайн магазини, поради което пробивът в тях не може да се свърже с хакерската атака към онлайн магазините. Посочено е още, че на 20.03.2025 г., 21.03.2025 г. и 10.04.2025 г. са получени имейли от анонимно лице, с което е поискан откуп с твърдение за осъществен неправомерен достъп.
В документа е отразено, че са взети следните мерки след първия инцидент: вътрешен одит на сигурността; промяна на паролите на вътрешнофирмените системи; промяна паролите на потребителите на Стеник, които имат достъп до административните панели; промяна на всички креденшъли на потребителите Стеник за публичната част на клиентските онлайн магазини; проверка на служебните компютри за вируси; уведомяване на клиентите за инцидента и даване на горепосочените две препоръки; провеждане на обучение на служителите на Стеник за опресняване знанията в областта на информационната сигурност. След втория инцидент са взети следните мерки: уведомяване на длъжностното лице за защита на лични данни; уведомяване на всички засегнати клиенти с имейл; извършване на одит за сигурността на сървърните системи (проверка на сървърния софтуер, проверка на достъп до сървър, като до нито един клиентски сървър не е имало неправомерен достъп; проверка за зловреден код, като такъв не е открит, проверка на мрежов трафик, като през цитирания от хакера период липсва аномалия в трафика, която да свидетелства за евентуален теч на данни); подаване на сигнал до ГДБОП; подаване на сигнал в КЗЛД; възобновяване на кампанията по активиране и настройване на двуфакторна автентикация за административните панели; преместване на пощенските кутии; закупуване и интегриране на нова Password manager; разширяване на вътрешните политики и инструктаж при фишинг.

В същия документ се съдържа информация за мрежовата връзка в офиса на жалбоподателя и ползваните компютри и софтуер от неговите служители.
По преписката са приложени писмо и списък на получатели (л. 499 – л. 505) за изпращане на 23.08.2025 г. на препоръка за активиране на двуфакторна автентикация. Такава препоръка е изпратена за втори път (05.03.2024 г.), видно от писмото и списък за получателите му (л. 506 – л. 512). През месец октомври 2024 г. жалбоподателят е изпратил до своите клиенти информация за потенциалните рискове от ползването на неактуална версия на платформата Magento Open Source (л. 513 – л. 517).
Представени са имейли на жалбоподателя, адресирани до клиенти, с които ги уведомяват за изпратения имейл от хакера и за възможния извършен неправомерен достъп до лични данни (л. 466 – л. 480 и л. 563 – л. 566).

Към преписката са приложени общи условия за предоставяне на услугата „Споделен хостинг“ от „Супер Хостинг Бг“ ЕООД (л. 542 –л. 557) и договор за предоставяне на информационни услуги (л. 559- л. 562).
Представени са Вътрешна инструкция за защита на личните данни на „Стеник груп“ ООД от 25.05.2018 г. (л. 94 – л. 101 и л. 457 – л. 460). В чл. 1, ал. 2 от инструкцията е регламентирано, че отговорно лице за защита на личните данни е управителят на дружеството. Според чл. 2, ал. 1 от Вътрешната инструкция дружеството събира, съхранява и обработва лични данни за своите партньори и клиенти с цел предоставяне на услуга и на основание сключен договор. На клиентите се предоставя подробна информация относно личните данни, които трябва да предоставят, целите, за които ще бъдат обработвани. Според чл. 2, ал. 2 данните на клиентите и партньорите се събират при сключване на договор с дружеството или при подготовка на такъв договор. Според чл. 18, ал. 1 дружеството използва хостинг компания за предоставяне на услугите си и поддържане на необходимата в тази връзка техническа инфраструктура при спазване на високи професионални стандарти, включително в областта на защита на личните данни. Съгласно чл. 18, ал. 2 достъпът до онлайн платформата на дружеството се извършва с име и парола, които се предоставят на служителите при постъпване на работа. Според чл. 20, ал. 1 личните данни, които дружеството събира и обработва, се съхраняват в електронни база данни с парола за достъп, която е предоставена единствено на определени служители с достъп до съответната категория лични данни.
Представени са Правила за политика на сигурността (л. 450 и л. 456), регламентиращи, че достъп до вътрешните електронни системи на Стеник, до външни електронни услуги използвани от Стеник и до клиентските онлайн магазини и системи се извършват само от служебен компютър на служителя. Развито са правила за работа с устройството, създаване на пароли и работа с електронна поща.
Посочено е, че при операция „Разработка на сайт и/или дендинг страница и поддръжка на сайт, профил, група или страница в социална мрежа“ (л. 441 и л. 455) се събират лични данни, каквито са определени в договора за възлагане на услугите от клиента към Стеник. Целите са следните: създаване на сайтове за нуждите на клиентите и провеждането на онлайн кампании за клиентите; предоставяне на поддръжка при функционирането на уебсайтовете; предаване на резултатите от проведени кампании.
Представен е регистър по чл. 30, параграф 2 от Регламент (ЕС) 2016/679 (л. 447), според който жалбоподателят съхранява и обработва лични данни на трети лица като част от предоставянето на услуги по договора за електронен магазин на конкретно посочени дружества. Приложение са още регистри по чл. 30, ал. 1 и чл. 31 от Регламент (ЕС) 2016/679.
По преписката е приложена молба от 06.11.2024 г. на „Стеник груп“ ООД, с която се отговоря на въпроси, поставени от проведената среща от 23.10.2024 г. и се представят следните документи: вътрешни материали за обучение (л. 257 – л. 277 и л. 391 – л. 398); декларация при постъпване на служител (л. 244); регистър на инциденти (л. 277); имейли към клиенти във връзка с инцидента (л. 359-л.362); имейли за активиране на двуфакторна защита от м. август 2023 г. и м. март 2024 г.; имейли от хакера (л. 346 – л. 358); сигнал до ГДБОП (л. 343 – л.345); екранни разпечатки - вход в Магенто, описание на таба с роли, информация за достъпа до сървъра; информация за одит на информационната сигурност (л. 326 – л. 342); структура на Стеник кой на каква машина работи; договор с хостинг компания и интернет доставчик (л. 299 – л. 325); заседания на GDPR борда (л. 281 – л. 298 и л. 399 – л. 416).
По преписката се намира детайлен анализ за въвеждане на GDPR на „Стеник груп“ ООД (л. 102-л.154).

Приложение са ГФО и ОПР за 2019 г., 2020 г., 2021 г. и 2022 г. на жалбоподателя.
Съставен е Констативен акт рег. № ПАИКД-13033-6/19.11.2024 г. от служители на КЗЛД, в който е възпроизведена информацията, отразена в уведомление от 01.04.2024 г., подадено от „Стеник груп“ ООД.
От протокол № 52/11.12.2024 г. се установява, че КЗЛД е провела заседание, на което са обсъдени становища след проверка, констативен акт от проверка, уведомление на жалбоподателя и доклад на Дирекция „ПАИКД“. На същото заседание е взето единодушно решение (4 гласували „за“) е прието, че жалбоподателят е извършил нарушение на чл. 5, пар. 1, б. „е“, вр. чл. 32, пар. 1, б. „б“ и б. „г“ и чл. 5, пар. 2 от Регламент 2016/679, при което на основание чл. 58, пар. 2, б. „г“ от Регламент 2016/679 е взето решение да се разпореди на „Стеник Груп“ ООД следното: 1. Да извършва анализ на риска, въз основа на който да определи подходящи технически и организационни мерки за защита на лични данни, между които: а). да регламентира извършването на периодична оценка на риска, въз основа на която да актуализира предприетите технически и организационни мерки за защита на личните данни; б). да извърши анализ на риска относно ползването на системи/приложения за съхраняване на пароли и съответно да опише предприетите технически и организационни мерки за преодоляване на констатирани рискове; в). да предвиди конкретни политики/правила/ процедура или други правни актове, които да регламентират обработването на лични данни чрез информационна система „Магнето“; г). да предвиди в своите вътрешни документи спазване на принципите на отчетност и извършване на периодичен одит с цел проверка на съответствието спрямо изискванията на Регламент 2016/679; д). да въведе политики и процедури за формиране и поддръжка на журнални записи (логове), за период, който да позволява спазването на принципа за отчетност, съгласно Регламент 2016/679; е). да предприеме необходимите действия за създаване на одитни записи на отделни събития и дневници (журнали) за привилегированите потребители (системни администратори); ж). да внедри Система за управление на привилегиите на потребителите и Система за управление и анализ на събитията, отразени в дневниците; 2. Да актуализира сключените договори със своите клиенти, в които да отрази приложените технически и организационни мерки, предприети въз основа на извършена оценка на риска.
На същото заседание е взето единодушно решение (4 гласували „за“) на основание чл. 58, апр. 2, б. „и“ от Регламент 2016/679 да се наложи на администратора на лични данни „Стеник груп“ ООд имуществена санкция в размер на 350 000 лева, съгласно чл. 83, пар. 4, б. „а“ за нарушение на чл. 32, пар. 1, б. „б“ и б. „г“, вр. чл. 5, пар. 1, б. „е“ от Регламент 2016/679 и чл. 83, пар. 5, б. „а“ за нарушение на чл. 5, пар. 2 от Регламент 2016/679.
Комисията за защита на личните данни се е произнесла с обжалваното Решение № ПАИКД-13-33/2024, с което на основание чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679 за нарушение на чл. 5, пар. 1, б. „е“, вр. чл. 32, пар. 1, б. „б“ и б. „г“ и чл. 5, пар. 2 от Регламент 2016/679 е разпоредено на жалбоподателя „Стеник груп“ ООД следното: 1. Да извършва анализ на риска, въз основа на който да определи подходящи технически и организационни мерки за защита на лични данни, между които: а). да регламентира извършването на периодична оценка на риска, въз основа на която да актуализира предприетите технически и организационни мерки за защита на личните данни; б). да извърши анализ на риска относно ползването на системи/приложения за съхраняване на пароли и съответно да опише предприетите технически и организационни мерки за преодоляване на констатирани рискове; в). да предвиди конкретни политики/правила/ процедура или други правни актове, които да регламенторат обработването на лични данни чрез информационна система „Магнето“; г). да предвиди в своите вътрешни документи спазване на принципите на отчетност и извършване на периодичен одит с цел проверка на съответствието

спрямо изискванията на Регламент 2016/679; д). да въведе политики и процедури за формиране и поддръжка на журнални записи (логове), за период, който да позволява спазването на принципа за отчетност, съгласно Регламент 2016/679; е). да предприеме необходимите действия за създаване на одитни записи на отделни събития и дневници (журнали) за привилегированите потребители (системни администратори); ж). да внедри Система за управление на привилегиите на потребителите и Система за управление и анализ на събитията, отразени в дневниците; 2. Да актуализира сключените договори със своите клиенти, в които да отрази приложените технически и организационни мерки, предприети въз основа на извършена оценка на риска. наредено е разпореждането да се изпълни в рамките на три месеца от влизане в сила ма решението, след което в 14- дневен срок да се уведоми КЗЛД.

С обжалваното Решение № ПАИКД-13-33/2024 г. на КЗЛД на основание чл. 58, апр. 2, б. „и“ от Регламент 2016/679 е наложена на „Стеник груп“ ООД, в качеството му на администратор на лични данни, имуществена санкция в размер на 350 000 лева, съгласно чл. 83, пар. 4, б. „а“ за нарушение на чл. 32, пар. 1, б. „б“ и б. „г“, вр. чл. 5, пар. 1, б. „е“ от Регламент 2016/679 и чл. 83, пар. 5, б. „а“ за нарушение на чл. 5, пар. 2 от Регламент 2016/679.

Органът е приел, че „Стеник груп“ ООД предоставя услуги по създаване и поддържане на Content management системи и платформи за онлайн магазини. На 05.03.2024 г. жалбоподателят бил информиран от портала за техническа поддръжка на хостинг услугите, че две от пощенските кутии на хостинг акаунта са използвани за изпращане на spam на други потребители. Впоследствие на 20.03.2024 г. жалбоподателят получава имейл от лице, представило се за „K. D.“, с покана за заплащане на откуп с твърдение, че в периода от 03 – 05 март 2024 г., чрез неправомерен достъп до административния панел на клиентите, е осъществен достъп до лични данни – имена, адреси, телефонни номера и имейли на клиенти на няколко онлайн магазини, чиято поддръжка се осъществява от „Стеник груп“ ООД.

Органът е обсъдил подробно процесуалните действия на своите служители и изпратената информация от жалбоподателя. Направен е извод за нарушение на поверителността на личните данни, състоящо се в нерегламентиран достъп до ползваните от „Стеник груп“ ООД административни панели на електронните магазини на негови клиенти. Вследствие на това нарушение, злонамерено лице е достъпило лични данни на близо 2 000 000 субекти, отнасящи се за имена, ЕГН, адреси и телефонен номер.

Органът е приел, че съгласно индивидуалните договори между съответните дружества – собственици на онлайн магазини и „Стеник груп“ ООД са изработени съответните електронни магазини и се осъществява тяхната поддръжка. Отношенията са регламентирани с договор за поддръжка на онлай магазини, при което съгласно чл. 8, пар. 8 от Регламент 2016/679 „Стеник груп“ ООД е „обработващ лични данни“. В приложение № 1 към договорите е отразено, че обработването на лични данни се извършва за следните цели: предоставяне на софтуер за електронен магазин; съхраняване на данни от потребителски профили и онлайн поръчки; предоставяне на техническа поддръжка. Посочено е, че според договорите „Стеник груп“ ООД преустановява достъпа до онлайн магазина, връща личните данни или същите се унищожават. Налице е позоваване на постъпила информация от 8 компании – бивши клиенти (не са посочени кои са дружествата), според която достъпът на Стеник до уеб сайтовете не е бил преустановен. На основание чл. 28, пар. 10 от Регламент 2016/679 е прието, че в този случай обработващият лични данни се счита за администратор на лични данни, т. е. Стеник няма действащи договори с тези дружества за обработване на лични данни, следователно Стеник сам определя целите и

средствата за обработване по отношение на тях.

По тези съображения е направен извод, че „Стеник груп“ ООД е администратор на лични данни по смисъла на чл. 4, пар. 7 от Регламент 2016/679 и е следвало да предприеме подходящи технически мерки и организационни мерки във връзка с изпълнение на собствените му функции и да гарантира сигурност на обработваните от него личните данни на физически лица във връзка с предмета си на дейност. Самостоятелно и на собствено основание е определял целите и средствата за обработване на лични данни при използване на различни приложения. Допуснато е нарушение на сигурността на лични данни за периода от 03.03.2024 г. – 21.03.2024 г., като не е извършен процес на редовно изпитване, преценяване и оценяване на ефективността на техническите и организационните мерки, за да се гарантира сигурността на обработването. Това е довело до невъзможност за приложение на подходящи мерки, вследствие на което е осъществен неоторизиран достъп и неразрешено разкриване на лични данни (имена, ЕГН, имейл, телефонен номер, адрес, пол и IP адрес) на 1 991 563 физически лица – клиенти на електронни магазини на дружествата, обслужвани от Стеник. По тези съображения е нарушен чл. 32, пар. 1, б. „б“ и б. „г“, вр. чл. 5, пар. 1, б. „е“ от Регламент 2016/679.

Съдържат се мотиви, според които системите за сигурност на успели да своевременно да информират Стеник за осъществения неоторизиран достъп до лични данни. Отхвърлят се възраженията, че двуфакторната автентификация е била въведена преди нарушението, с което е нарушен чл. 5, пар. 1, б. „е“, вр. чл. 32, пар. 1, б. „б“ от Регламент 2016/679.

Пояснява се за липсата на въведени подходящи технически и организационни мерки за защита на личните данни и липсата на предварително реално извършена оценка на риска. Последната не обхващала в пълнота процесите по обработване на лични данни, доколкото не е установен конкретния неправомерен достъп и как е осъществен нерегламентираното достъпване на лични данни. По този начин е нарушен чл. 32, пар. 1, б. „г“ от Регламент 2016/679.

Развити са съображения, че Стеник не е доказал спазването на чл. 5, пар. 1 от Регламент 2016/679, като по този начин е нарушен принципа за отчетност по чл. 5, пар. 2 от Регламент 2016/679, т. е. не са представени вътрешни документи/политики, които да регламентират обработване на лични данни чрез ползването на информационна система „Магенто“.

Допълнително в мотивите са развито съображения за определяне на размера на имуществената санкция.

В съдебно заседание са представени протоколи от проведени GDPR бордове. Декларации за конфиденциалност на служители на „Стеник груп“ ООД и доказателства за прочениетни имейли, изпратени от жалбоподателя по повод изпратени препоръки през 2023 г. за активиране на двуфакторна автентикация.

В съдебно заседание са представени документи, отнасящи се за извършена от КЗЛД проверка на 11 броя търговски дружества, които са собственици на електронни магазини: „Би фит“ ООД, „Витаслим инове“ ООД, „8 Е.“ ЕООД, „Евро пест“, „Мувио лоджистик“ ЕООД. „Айко мулти консепт“ ООД, „Хиполенд“ АД, „Скайшоп България“ ЕООД, „Парфюмери дъглас България“ ЕООД, „Теодор“ ООД и „Лили дрогерие“ ЕООД. Същите имат сключени договори със „Стеник груп“ ООД, отнасящи се за поддръжка на електронните магазини. Отделно от това с жалбоподателя са сключени договори за обработка на лични данни.

Договорите за обработка на лични данни са типови, респ. идентични за всички 11 търговски дружества, собственици на електронни магазини. В същите е уговорено, че администраторът на лични данни, представляващ собственик на съответния електронен магазин, е възложил на „Стеник груп“ ООД обработването на лични данни под контрола на администратора на лични

данни. Личните данни се обработват в съответствие с инструкциите на администратора и изискванията на Приложение № 1. С договора обработващият лични данни декларира, че е въвел изискванията на Регламент 2016/679 в своята дейност, включително технически и организационни мерки за защита на лични данни.
В приложение № 1 към договорите за обработка на лични данни е посочено, че обработващият е разработил и поддържа електронен магазин, който се предоставя за ползване на администратора. Обработването на лични данни от обработващия се извършва за следните цели: предоставяне на софтуер за електронен магазин; съхраняване на данни от потребителски профили и онлайн поръчки; предоставяне на техническа поддръжка. Срокът за обработка е за срока на договорите за предоставяне на поддръжка на електронен магазин. Категорията субекти на данни са физическите лица – клиенти на администратора. Видовете лични данни са следните: три имена, ЕГН, имейл, телефонен номер и адрес.
В приложение № 2 към договорите за обработка на лични данни са посочени технически и организационни мерки за защита на лични данни, които се задължава жалбоподателят да спазва при обработката на лични данни.
Представени са договори за поддръжка, сключени между „Стеник груп“ ООД и с част от съответните дружества - собственици на онлайн магазини, с които жалбоподателят съдейства за отстраняването на възникнали проблеми по електронния магазин.
Приложени са още договори за изработка на уеб сайт, сключени между „Стеник груп“ ООД и с част от съответните дружества - собственици на онлайн магазини.
По делото е изслушано заключение на съдебно – компютърна и техническа експертиза, което съдът кредитора, тъй като е обосновано и непротиворечиво.
Експертът разяснява, че действията, които се извършват в системите на дружеството могат да бъдат проследени до 5 дни назад във времето, т. е. т. нареченият back up се прави за период от 5 дни. В тази връзка не е възможно да се установи дали е осъществен достъп или не е осъществен достъп до лични данни. Дружеството прилага стандартни технически мерки за сигурност като CDN, WAF, DDOS, Malware scanner и Jumphost. Въведена е още специална мярка за обезпечаване на сигурния достъп на собствениците на електронни магазини, а именно двуфакторна автентификация за достъп до административните панели на онлайн магазини, което е извършено през 2023 г. същата била достатъчна с оглед достиженията на техническия прогрес. Отделно от това за взети организационни мерки (GDPR борд в дружеството, протоколи от заседания на този борд, вътрешни правила за защита на лични даннипри поддръжка на електронни магазини, регистър за обучените служители за работа с лични данни и регистър на лицата с достъп до лични данни), които според вещото лице гарантират висока степен на поверителност, цялостност, наличност, устойчивост и сигурност при обработване на лични данни. Уточнява, че не е възможна 100 % защита от неоторизиран достъп.
Експертът посочва, че администраторските панели, през които се достъпват онлайн магазините и през които има достъп до личните данни на клиентите на магазините, се предоставят за управление от собствениците на тези онлайн магазини, които са клиенти на Стеник. Достъпът на оторизирани служители на Стеник се осъществява през този администраторски панел чрез предоставен на Стеник т. нар. съпорт акаунт “stenik“ (достъп за осъществяване на поддръжка). Същият се предоставя за определен период за извършване на конкретна задача по поддръжка. Уточнява, че съобразно практиката на дружеството този период е до края на работния ден, след което акаунта се деактивира, а ако задачата не е била приключена, то на следващия работен ден се активира нов акаунт.
При така установените факти, съдът достига до следните правни изводи:

Жалбата е подадена в срок, от лице, което е адресат на акта, който е неблагоприятен за него, поради което е налице правен интерес от оспорването.
Съгласно изискванията на чл. 168, ал. 1 АПК, при служебния и цялостен съдебен контрол за законосъобразност, съдът извършва пълна проверка на обжалвания административен акт относно валидността му, спазването на процесуалноправните и материалноправните разпоредби по издаването му и съобразен ли е с целта, която преследва законът, т. е. на всички основания, визирани в чл. 146 АПК. При преценката си, съдът изхожда от правните и фактическите основания, посочени в оспорвания индивидуален административен акт, представената административна преписка и събраните по делото доказателства. При проверката на административния акт, съдът не е обвързан от основанията, въведени от оспорващия, нито от неговото искане.
Разгледана по същество, жалбата е основателна по следните съображения:
Обжалваното решение е издадено от компетентен колективен орган съгласно чл. 38, ал. 3 от ЗЗЛД, 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 за дейността на КЗЛД и нейната администрация). Съгласно чл. 7, ал. 1 ЗЗЛД комисията е колегиален орган и се състои от председател и 4 членове, а решенията се вземат с мнозинство от общия брой на членовете ѝ (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 налице отменителното основание 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 реквизити по чл. 59, ал. 2 АПК. Оспореният акт съдържа ясна разпоредителна част и са посочени релевантните факти и обстоятелства, послужили за обявяване на жалбата за основателна.
Допуснати са съществени процесуални нарушения.
Най – напред следва да се посочи, че не се споделят възражения на жалбоподателя за липсата на доказателства за осъществен пробив в електронната система, управляваща онлайн магазините, обслужвани от Стеник. Това е така, тъй като с писмо от 01.04.2024 г. (л. 90- л. 93 гръб по делото), подписано от представител на дружеството – жалбоподател, се признават конкретни факти, свързани с техническия механизъм на осъществен пробив в системата. В тази връзка се признава, че е разбит фирмения G. Password Manager на Стеник (съдържащ към онзи момент пароли за клиентски административни панели), посредством хакване на компютър на служител на жалбоподателя. Осъществен е достъп до административните панели с потребителски имена и пароли, ползвани от Стеник, а именно през акаунта на жалбоподателя с username stenik (логин в административния панел). Посочено признание на факт се подкрепя и от заключението на експертизата, според което достъпът на оторизирани служители на Стеник се осъществява през този администраторски панел чрез предоставен на Стеник т. нар. съпорт акаунт “stenik“. Обсъжданият документ от 01.04.2024 г. съдържа извънсъдебно признат неизгоден факт, поради което се ползва с обвързваща съда доказателствена сила.
Горното води до извод за неоснователност на възраженията, свързани с уведомяването на собствениците на онлайн магазини за активиране на двуфакторна автентификация, тъй като пробивът е осъществен от компютър на служител на жалбоподателя, а не от чуждо устройство (на собственик на онлайн магазин).
Важно е да се уточни, че писмото от 01.04.2024 г. съдържа признание за осъществен пробив в съответната електронна система, но не се признават факти дали е осъществен достъп до лични

данни, изтичане на лични данни, техния вид и количество. Единствено са изложени предположения за вида на личните данни, до които е възможно да е осъществен достъп. По тези съображения в тази част документът не се ползва с доказателствена сила, при което органът има задължение да установи тези факти.
В оспореният акт се поддържа за осъществен достъп на лични данни на близо 2 000 000 субекти, отнасящи се за имена, ЕГН, адреси и телефонен номер. Не става ясно по какъв начин е установен видът и количеството лични данни, доколкото не са събрани никакви доказателства в тази насока. Вероятно тези факти се извеждат от писма на жалбоподателя, но същите по отношение на тези факти не представляват признание на факти, а единствено предположения, т. е. органът е направил изводи за вида и количеството лични данни на база предположения. Органът въобще не е обсъдил и изследвал факти, отнасящи се за значението на административния панел на онлайн магазините, т. е. дали пробивът в тях води до базата данни, съдържаща лични данни на клиенти на магазините. Следва да се обоснове и докаже връзката между административния панел и базата данни, съдържаща лични данни, което в случая не е направено. Това е така, тъй като не всеки пробив на дадена система води категорично до достъп до лични данни, доколкото е възможно пробивът да е свързан с други функции на системата, различаваща се от съхранението на лични данни. По тези съображения органът не е изяснил както наличието на осъществен достъп до лични данни, така и техния вид и количество. Изводите на органа за тези факти не се подкрепят с никакви доказателства, събрани в производството, при което са нарушени чл. 35 и чл. 36 АПК. Изясняването на тези факти е от първостепенно значение за това дали са нарушени сочените от органа норми от Регламент 2016/679, поради което обсъжданото нарушение на чл. 35 и чл. 36 АПК се отразява на приложението на закона, поради което е налице допуснато съществено процесуално нарушение по смисъла на чл. 146, т. 3 АПК, водещо до незаконосъобразност на оспорения административен акт.
Нарушение на чл. 35 и чл. 36 АПК е допуснато и по отношение изясняването правоотношенията между Стеник и неговите клиенти – собственици на електронни магазини. Органът прави извод, че на основание чл. 28, пар. 10 от Регламент 2016/679 жалбоподателят е администратор на лични данни, което се прави единствено и само на база постъпила информация от 8 компании – бивши клиенти, според която достъпът на Стеник до уеб сайтовете не е бил преустановен, т. е. Стеник няма действащи договори с тези дружества за обработване на лични данни, следователно жалбоподателят сам е определя целите и средствата за обработване по отношение на тях. Органът не е посочил кои са тези 8 дружества, което препятства възможността да се прецени дали са налице действащи или прекратени договори за поддръжка на онлайн сайт, както и дали личните данни на потребителите на стоки/услуги на тези електронни магазини са обект на неправомерен достъп. Освен това органът не е съобразил, че ако се приеме за достоверна информацията на тези 8 дружества, то изводът за приложението на чл. 28, пар. 10 от Регламент 2016/679 не би могъл да се направи спрямо останалите клиенти на жалбоподателя, с които е налице сключен договор за поддръжка на онлайн магазин. В., органът въобще не е изяснил кои са действащите и кои са прекратените договори, сключени между Стеник и собствениците на електронни магазини. В тази връзка не е изяснен срокът на действие на обработване, което е от значение съгласно чл. 28, пар. 3 от Регламент 2016/679. Основателно възниква въпросът – как е осъществяван достъп (предоставен акаунт за достъп) до онлайн магазини при положение, че са прекратени договорите за поддръжка. Отговор на такъв въпрос не е даден от органа и не са изяснени тези обстоятелства. Липсва всестранно изследване на фактите, тъй като органът се е позовал на информация на 8 дружества (без да сочи кои), но не е проверил дали същата отговоря на действителното положение. Не може да се отмине и фактът, че въобще не е индивидуализирана тази информация

– кога и от кое лице е подадена, включително по кое производство, тъй като в представеното пред съда писмо от 24.11.2025 г. се поддържа за 11 образувани преписки, т. е. същите да са отделни от преписката, по която е издадено оспореното решение. Освен това, не е дадена възможност на жалбоподателя да се запознае с тази информация и да изрази становище по случая, с което е нарушено правото на жалбоподателя за участие в производството. Неизясняването на всички обсъдените факти и обстоятелства има значение за приложението на нормата на чл. 28, пар. 10 от Регламент 2016/679, според която без да се засягат членове 82, 83 и 84, ако обработващ лични данни наруши настоящия регламент, определяйки целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване. По тези съображения неизясняването на обсъжданите факти е довело до съществено процесуално нарушение по смисъла на чл. 146, т. 3 АПК, което води до незаконосъобразност на оспорения административен акт.

По горните съображения се налага извод за основателност на жалбата, поради което следва да се отмени оспореното решение.

По разноските:

С оглед изхода на делото и на основание чл. 143, ал. 1 АПК следва да се присъдят направените разноски от жалбоподателя, които са следните: 50 лева (25,56 евро) – държавна такса, 782 лева (399,83 евро) – депозит за вещо лице и 22 380 лева (11 442,71 евро) – адвокатски хонорар, видно от договора за равна помощ и документи за изплащането му.

Основателно е възражението за прекомерност на адвокатски хонорар. В чл. 8, ал. 1, т. 10 от Наредба № 1/09.07.2004 г. е регламентирано, че минималният размер на адвокатски хонорар за дела по Закона за защита на личните данни е 900 лева. За да е справедливо и обосновано, заплатеното адвокатско възнаграждение следва да отчита обстоятелствата, характеризиращи конкретното дело, сред които са видът и количеството на осъществената в полза на страната, претендираща разноски, правна помощ, фактическата и правна сложност на делото, както и продължителността на процеса. Проведени са пет заседания, изслушано е едно заключение на експертиза, а обемът на доказателствата не е малък, поради което делото се отличава със средна към голяма сложност от фактическа страна. Същото се отнася и за правна страна, тъй като се налага съобразяване на редица правни норми. В тази връзка възнаграждението за адвокат следва да се намали до 2 500 евро, т. е общият размер на всички разноски е 2 925,39 евро.

По изложените съображения, съдът

Р Е Ш И:

ОТМЕНЯ Решение № ПАИКД-13-33/2024 на Комисията за защита на личните данни.

ОСЪЖДА Комисията за защита на личните данни да заплати на „Стеник груп“ ООД сумата в размер на 2925,39 евро, представляваща направени разноски.

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

Съдия: