Р Е Ш Е Н И Е
№ 26579

гр. София, 10.12.2024 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 56 състав,** в публично заседание на 25.09.2024 г. в следния състав:

СЪДИЯ: Мария Ситнилска

при участието на секретаря Макрина Христова, като разгледа дело номер **4207** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 126 и сл. от Административно процесуалния кодекс във връзка с чл. 84, ал. 2 от Закона за защита на личните данни.

Образувано е по жалбата на Пенсионноосигурително дружество "ТОПЛИНА"АД, ЕИК[ЕИК], представлявано от Г. П. Л. и С. Т. Г. чрез пълномощник адв. К. Д. против решение № ПАИКД-13-7/23 от 28.02.2024 г. на Комисията за защита на личните данни в частта му, с която на основание чл. 58, §2, б. „и" от Регламент (ЕС)2016/679 на дружеството е наложено административно наказание - имуществена санкция в размер на 20 000 лева, съгласно чл. 83, §4, б. „а" за нарушение на чл. 24, ал. 1, чл. 25, ал. 1, чл. 32, § 1, б. „б" и б. „г" от Регламент (ЕС) 2016/679 и чл. 83, § 5, б. „а" за нарушение на чл. 5, § 1, б. „е" от Регламент (ЕС)2016/679. Обосновават се твърдения за незаконосъобразност на оспореното решение, поради съществено нарушение на административно производствените правила, противоречие с материално правните разпоредби и несъответствие с целта на закона. Излагат се доводи, че е недопустимо с индивидуален административен акт, какъвто характер има оспореното решение, да се налага административно наказание. Посочва се, че в чл. 58 от Регламент (ЕС) 2016/679 са установени правомощията на надзорните органи да прилагат принудителни административни мерки и да налагат административни наказания, но процедурите за реализирането им се урежда в националните законодателства на държавите членки. В българското право за принудителните административни мерки се прилага чл. 84 от ЗЗЛД и съответно АПК, а за административно наказателната

отговорност - чл. 87 от ЗЗЛД и съответно правилата на ЗАНН. Позовава се на чл. 87 от ЗЗЛД, където е посочено, че установяването на нарушенията на Регламента или на ЗЗЛД, издаването, обжалването и изпълнението на наказателните постановления се извършва по реда на ЗАНН. Сочи се, че в процесния казус изобщо не е спазена предвидената в закона процедура, като не е съставен АУАН и не е издадено наказателно постановление, поради което наложената имуществена санкция е незаконосъобразна и само на това основание е достатъчно решението на КЗЛД да бъде отменено в обжалваната му част. Излагат се доводи, че дружеството е предприело всички необходими мерки, съгласувани с КЗЛД и ГДБОП, сайтът на дружеството – обект на хакерска атака, да бъде изключен и да стане изцяло недостъпен, без да бъдат правени опити за неговото стартиране. Като безспорен се изтъква фактът, че от момента на инцидента до настоящия момент няма постъпила нито една жалба или сигнал от клиенти засегнати от хакерската атака за злоупотреба с личните им данни. Моли съда да постанови решение, с което да отмени решението в оспорената му част. Претендира разноски.

Ответникът - Комисията за защита на личните данни, в депозирано по делото писмено становище оспорва жалбата. Като неоснователен се оспорва доводът на санкционираното дружество, че административното наказание имуществена санкция може да бъде наложено с решение на КЗЛД единствено в хипотезата на чл. 38, ал. 1 от ЗЗЛД. Изтъква се, че в практиката безспорно е установена възможността предвидените административни наказания да бъдат налагани, както в рамките на производството по реда на ЗАНН, така и по реда на АПК, когато КЗЛД действа като колективен административен орган, чиито актове се оспорват по реда на АПК. Излагат се съображения, че упражняването от надзорния орган на санкционните правомощия по Регламент (ЕС)2016/679 не е пряко обвързан с предприетите в последствие действия от администратора мерки за защита на личните данни. Същите се вземат предвид от надзорния орган единствено като смекчаващи или утежняващи вината обстоятелства. Претендира се отхвърляне на жалбата и присъждане на юрисконсултско възнаграждение. Прави възражение по чл. 78, ал. 5 от ГПК.

Административен съд София-град, като взе предвид изложеното в жалбата и представените по делото писмени доказателства, прие за установено от фактическа страна следното:

Административното производство пред Комисията за защита на личните данни е образувано по повод постъпило от ПОД „Топлина“АД Уведомление за нарушаване на сигурността на данните вх. № ПАИКД-13-7/17.02.2023 г. В същото се съдържа информация, че на 15.02.2023 г., в 09.21 ч., на официалния имейл на дружеството [електронна поща] е получено писмо на английски език от адрес [електронна поща] съдържащо информация, че от водените от дружеството електронни регистри са източени 161 записа, отнасящи се до личните данни на лица, като е посочена извадка и таблица с цитиране на около 20 записа, съдържащи лични данни на осигурени лица в управляваните от дружеството фондове за допълнително пенсионно осигуряване. С писмото е поискан откуп и е отправена заплаха за нанасяне на репутационни вреди. При направена проверка на посочените в писмото данни е установено, че данните съвпадат с тези от водените от дружеството регистри, като информацията е извлечена през стария електронен сайт на ПОД „Топлина“ АД. Посочва се, че на официалната интернет страница на дружеството има функционалност, която позволява осигурените лица да получат достъп до състоянието и движението по индивидуалните им

осигурителни партиди във фондовете за допълнително пенсионно осигуряване чрез предоставени потребителско име и парола. Дружеството има нова електронна страница, като достъпът до старата е бил запазен, тъй като по технически причини достъпът до новия сайт за вече регистрирани лица, може да стане единствено чрез посещение на новия и настоящ, от който е наличен препращащ линк към стария сайт. Уточнено е, че информацията, до която е получен достъп и която е неправомерно извлечена, е от базата данни на стария сайт, който чрез API извлича данни в статус READ ONLY от реалната база, пазеща всички регистри с информация за осигурените лица и техните парични потоци.

С писмо № ПАИКД-13-7#1/14.03.2023 г. от КЗЛД е изискана допълнителна информация от ПОД „Топлина“ АД с оглед изясняване на фактите и обстоятелствата посочени в уведомлението.

С писмо № ПАИКД-13-7#2/17.03.2023 г. дружеството е предоставило исканата информация на КЗЛД. В писмото се посочва, че в резултат на прегледаните журнали, касаещи достъпа до стария сайт, е направено предположение, че при хакерската атака е използвана уязвимост в PHP технологията, с която е изработен. В тази база данни не се съхраняват финансови данни. Те се предоставят само докато е активна дадена сесия на влязъл потребител в свия акаунт. При излизане от акаунта, финансовите данни към дадено лице вече не са налични и не се съхраняват на стария сайт. Финансовите данни на осигурените лица се съхраняват само в електронните регистри (реалната база данни) поддържани от „А.К.Т.А“ООД (разработчик на програмата), която не е засегнати. Личните данни на регистрираните потребители в новия сайт не са засегнати от конкретния инцидент. Достъпът до стария сайт е преустановен незабавно след узнаване на инцидента на 15.02.2023 г. Към писмото са приложени: заповед № 20/16.02.2023 г. за определяне на Комисия за извършване на проверка; протокол от 22.02.2023 г. с приложенията към него за извършена проверка на инцидент № IR-2023-001/15.02.2023 г.; договор с „ИНТЕПРО Солюшънс“ ООД за поддръжка на системи за сигурност № S102/01.05.2009 г.; Оценка и анализ на риска по отношение на нарушението на сигурността на данните от 23.02.2023 г.; Правилник за защита и обработване на личните данни на ПОД „Топлина“ АД, приет с решение на Управителния съвет от 21.05.2018 г, както и Методика на ПОД „Топлина“ АД за определяне на нивото на риска при нарушения на сигурността на личните данни. В протокола за извършена проверка е посочено, че данните засегнати от нарушението са както следва: ЕГН, три имена, адрес електронна поща - 109 406 лица и ЕГН, фамилия и инициали за име и презиме, адрес и електронна поща -12015 лица.

С докладна записка № ПАИКД-13-7#3/27.03.2023 г. постъпилото Уведомление е докладвано на заседание на КЗЛД, проведено на 29.03.2023 г. Взето е решение да бъде извършена проверка на място, поради наличие на „високо ниво на риск“ за правата и свободите на физическите лица.

Със заповед № РД-15-04/08.01.2024 г. на председателя на КЗЛД е разпоредено извършване на проверка на място.

За разпоредената проверка ПОД „Топлина“АД е уведомено с писмо №ПАИКД-13-7#6/11.08.2023 г.

Проверката на място е извършена на 23.01.2024 г. в административната сграда на ПОД „Топлина“. По време на проверката е демонстрирана функционалността на новия сайт на дружеството и достъпът до собствените партиди на клиентите посредством потребителско име (индивидуален осигурителен номер на партидата) и

парола (ЕГН). Установено е, че след успешен вход в системата се визуализира единствено натрупаната сума до момента по партидата на клиента в съответните пенсионни фондове, но не и лични данни, както и липсва възможност за промяна на потребителското име и паролата. Не е извършена проверка на функционалността на стария сайт на дружеството, през който е извлечена информацията, предмет на хакерската атака, тъй като от страна на ПОД „Топлина“АД са изложени твърдения, че след инцидента старият сайт на дружеството е изцяло недостъпен, сървърът на който е качен е изключен и от съображения за информационна сигурност не са правени опити за неговото стартиране. В хода на проверката е установено, че в изпълнение на заповед № 20/16.02.2023 г. на председателя и заместник-председателя на Управителния съвет на ПОД „Топлина“ е извършена проверка по повод инцидента от служители на дружеството, за което е изготвен протокол от 22.02.2023 г. Установено е, че информацията е извлечена през стария сайт на дружеството на 14.02.2023 г. между 15-17 ч. Личните данни на осигурените лица, които се съдържат в извлечените таблици са следните: потребителско име, парола в шифрован вид с приложен „salt“, имена, ЕГН, адрес и електронен адрес. Не са достъпени и извлечени финансови данни на осигурените лица, както и друг вид информация, свързана с тяхното осигуряване, тъй като в базата данни на стария сайт, която е засегната от инцидента, не се съхраняват финансови данни. Те се предоставят само докато е активна дадена сесия на влязъл потребител в неговия акаунт. Броят на засегнатите от инцидента записи на лични данни от таблица „Users“ в резултат на хакерската атака са 160 230. Засегнати от нарушението са 121 421 осигурени във фондове за допълнително пенсионно осигуряване лица над 18 г., от които 2 987 лица са починали. Броят записи е по-голям, поради факта, че едно лице може да се осигурява в повече от един фонд, управляван от дружеството. В броя записи има повтаряемост на лица, в зависимост от това дали имат повече от една партида. Категориите данни на общо физическите лица, засегнати от нарушението са както следва: ЕГН, три имена, електронна поща - 109 406 лица, ЕГН, фамилия и инициали за име и презиме, адрес, електронна поща - 12 015 лица.

Резултатите от проверката са обективирани в Констативен акт № ППН-02-98/14.02.2024 г.

Изготвено е становище рег. № ПАИКД-13-7#9(23)/27.04.2024 г. Обоснован е извод, че ПОД „Топлина“АД в качеството на администратор на лични данни по смисъл на чл. 4, т. 7 от Регламент (ЕС) 2016/679 е допуснал нарушаване на сигурността при осъществяване на дейността си, а именно: било е възможно трети лица да изтеглят 161 хиляди записа, отнасящи се до лица, клиенти на дружеството. Прието е, че описаното нарушение на сигурността в Уведомление за нарушение на сигурността № ПАИКД-13-7/17.02.2023 г. показва, че администраторът не е предприел достатъчни технически и организационни мерки, които да гарантират подходящо ниво на сигурност на личните данни, предоставени от клиенти на администратора. За старият сайт администраторът не е предоставил доказателства за предприемане на необходимите, съгласно чл. 32, § 1, б. „г“ от Регламента процеси на редовно изпитване, преценяване и оценка на ефективността на предприетите технически и организационни мерки, които да гарантират сигурността на обработването на личните данни. На практика дружеството е уведомено за осъществения нерегламентиран достъп от трета страна, като приложените от него инструменти за сигурност не са отбелязали и сигнализирали за нарушението.

С решение по протокол № 8 от 28.02.2024 г. КЗЛД е приела становище рег. № ПАИКД-13-7#9 (23)/27.04.2024 г., определила е административно наказание - имуществена санкция в размер на 20 000 лева и е издала разпореждане на дружеството по чл. 58, § 2, б. и „г“ от Регламент (ЕС) 2016/679.
Въз основа на така проведеното административно производство, Комисията за защита на личните данни е издала решение № ПАИКД-13-7/2023 от 28.02.2024 г., с което:
на основание чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679 за нарушение на чл. 5, § 1, б. „е“ във връзка с чл. 32, § 1, б. „б“ Регламент (ЕС) 2016/679 е разпоредено на администратора на лични данни ПОД„Топлина“ АД с цел създаване на сигурни пароли на клиентите, заявили достъп до функционалността, която дава възможност да се провери състоянието по индивидуалната осигурителна партида, след първоначалното влизане с определената служебна парола - ЕГН, по-нататъшния достъп до системата да изисква от страна на клиента задължителна смяна на паролата.
на основание чл. 58, § 2, б. „и“ от Регламент (ЕС) 2016/679 на администратора на лични данни ПОД „Топлина“АД е наложено административно наказание - имуществена санкция в размер на 20 000 лева, съгласно чл. 83, §4, б. „а“ за нарушение на чл. 24, ал. 1, чл. 25, ал. 1, чл. 32, § 1, б. „б“ и б. „г“ от Регламент (ЕС) 2016/679 и чл. 83, § 5, б. „а“ за нарушение на чл. 5, § 1, б. „е“ от Регламент (ЕС) 2016/679.
От фактическа страна решението е мотивирано с това, че администраторът на лични данни ПОД „Топлина“АД е допуснал възможност да се осъществи неразрешен, преднамерен достъп до лични данни, обработвани чрез стария сайт на администратора, като не е предприел необходимите технически и организационни мерки и по този начин трети лица са имали достъп до данни за 121 421 физически лица над 18 години - субекти на лични данни, осигурени във фондовете за допълнително пенсионно осигуряване, от които 2987 лица са починали. Комбинацията от лични данни, до които третите лица са имали достъп, позволява засегнатите субекти на данни да бъдат идентифицирани лесно, без да са необходими допълнителна информация и специални механизми за обработване: имена, ЕГН, адрес и адрес на електронна поща.
Въз основа на така установеното от фактическа страна настоящият съдебен състав обосновава следните правни изводи:
Жалбата е ПРОЦЕСУАЛНО ДОПУСТИМА, като подадена в срок, от легитимирано за това лице и срещу подлежащ на оспорване индивидуален административен акт. Съобщението за постановеното решение е получено на 08.04.2024 г., а жалбата е подадена до административния орган на 19.04.2024 г.
Разгледана по същество жалбата е НЕОСНОВАТЕЛНА по следните съображения:
Оспореният административен акт е издаден от компетентен административен орган в рамките на законоустановените му правомощия.
Нормата на чл. 6, ал. 1 от ЗЗЛД постановява, че 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.
Съгласно чл. 10 от ЗЗЛД, КЗЛД изпълнява задачите по чл. 57 от Регламент (ЕС) 2016/679. Правомощието на КЗЛД за извършване на проверки е регламентирано изрично в нормата на чл. 12 от ЗЗЛД, съгласно която, председателят и членовете на комисията или

упълномощени лица от администрацията й, осъществяват контрол чрез проверки за спазване на Регламент /ЕС/ 2016/679. В текста на чл. 33 от Регламент (ЕС) 2016/679 е посочено, че в случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и, когато това е осъществимо - не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни надзорния орган, компетентен в съответствие с член 55, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа. В чл. 55 от Регламент /ЕС/ 2016/679 е посочено, че всеки надзорен орган е компетентен да изпълнява задачите и да упражнява правомощията, възложени му в съответствие с регламента, на територията на своята собствена държава членка. На територията на Р. България, надзорен орган по защита на личните данни е КЗЛД, съгласно чл. 10 от ЗЗЛД, както беше посочено, която с оспореното решение е упражнила своите правомощия по чл. 58, § 2 от Регламент /ЕС/ 2016/679. Т.е., доколкото комисията е сезирана с уведомлението за наличие на нарушение ЗЗЛД, то в нейните правомощия е да се произнесе с решение, което подлежи на оспорване пред административния съд. На основание чл. 9, ал. 4 във връзка с ал. 3 от ЗЗЛД решенията на Комисията се вземат с мнозинство от общия брой на членовете й, който съгласно чл. 7, ал. 1 от ЗЗЛД и чл. 4, ал. 1 от Правилника е председател и 4-ма членове при проведено открито заседание. След като изрично не е посочен вида на мнозинството, се приема, че то е обикновено, а не квалифицирано. Правилата за кворума и мнозинството са изложени в чл. 8, ал. 6 и ал. 7 от ПДКЗЛДНА: заседанията на Комисията се провеждат, ако на тях присъстват най-малко трима от нейния състав. Комисията взема решения чрез явно гласуване с мнозинство от три гласа. На проведеното на 28.02.2024 г. заседание на КЗЛД, когато е взето оспореното в настоящото съдебно производство решение, са присъствали трима от членовете на Комисията. Решението е прието с мнозинство, като трите гласа са достатъчни по закон. Предвид това, настоящият съдебен състав намира, че актът е постановен от компетентен орган и не е налице отменителното основание по чл. 146, т. 1 от АПК.

Административният акт е издаден в изискуемата писмена форма и е обективиран като решение, съгласно изискването на закона. Решението съдържа всички изискуеми реквизити, предвидени в чл. 59, ал. 2 от АПК, включително фактическите и правни основания за негово издаване. Волята на органа е обективирана в диспозитивната част, като решението

съответства на изложените мотиви. Не се доказва наличие на порок във формата на акта, представляващ самостоятелно основание за неговата отмяна по смисъла на чл. 146, т. 2 във връзка с чл. 59, ал. 2, т. 4 от АПК.
В настоящият случай, административното производство по издаване на оспореното решение е започнало по подадено на основание чл. 33 от Регламент (ЕС) 2016/679, Уведомление за нарушение на сигурността на личните данни. Редът за разглеждане на уведомлението е разписан в Правилника за дейността на КЗЛД и нейната администрация (раздел VII, чл. 62 и чл. 63) и същия е различен от този по Раздел II от ППКЗЛДНА във връзка с чл. 38 и сл. от ЗЗЛД. Съгласно цитираните разпоредби, след регистриране на уведомлението, съответната дирекция, в едномесечен срок извършва анализ на постъпилата информация за пълнота на данните по чл. 33, §3 от Регламент (ЕС) 2016/679, съответно чл. 67, ал. 3 от ЗЗЛД, при който се изясняват конкретни въпроси, в това число се определя нивото на риска. След това се изготвя мотивиран доклад от дирекцията до КЗЛД с предложения, в т.ч. за извършване на проверка по документи или на място, съобразно предложеното ниво на риск. За решението на Комисията се уведомява администраторът, а при необходимост и други, свързани с нарушението, страни. В случая, на заседание, проведено на 29.03.2023 г. е взето решение за извършване на проверка на място, за което решение жалбоподателят е уведомен с писмо №ПАИКД-13-7#6/11.08.2023 г. Резултатите от проверката са обективирани в Констативен акт № ППН-02-98/14.02.2024 г.
След приключване на проверката, КЗЛД е взела решението си, съгласно чл. 63, ал. 3 от Правилника за дейността на КЗЛД, на свое заседание, проведено на 28.02.2024 г., за което е съставен протокол № 8.
Не се споделят доводите на оспорващото търговско дружество, че в случая са приложими нормите на Закона за административните нарушения и наказания (ЗАНН). С разпоредбата на чл. 12 от ЗЗЛД, на председателя и членове на комисията или на упълномощени от тях лица от администрацията са възложени правомощия за осъществяване на контрол чрез предварителни консултации, проверки и съвместни операции за спазване на Регламент (ЕС) 2016/679 и на този закон, които съгласно чл. 12, ал. 7 от ЗЗЛД завършват с констативен акт, като в случаите, когато е установено нарушение констативният акт е акт за установяване на административното нарушение по смисъла на ЗАНН. От анализа на посочените законови разпоредби се стига до извода, че органите, които осъществяват контрол за спазване на Регламент (ЕС) 2016/679 са: 1 / Комисията на основание чл. 10, ал. 1, т. 7 по реда на чл. 38 и чл. 39 от ЗЗЛД и 2 / Председателят на КЗЛД и членовете на комисията

или упълномощени от тях лица от администрацията на основание чл. 12 от ЗЗЛД.

Редът, по който се осъществяват двата вида контрол е различен. Когато Комисията е сезирана с жалба /сигнал/ от физическо лице, което твърди, че са му нарушени правата по ЗЗЛД, тя се произнася, съгласно чл. 38, ал. 2 с решение, какъвто е конкретният случай. Съгласно дадените от закона в този случай правомощия тя постановява решение, с което може: а/ да даде задължителни предписания, б/ да определи срок за отстраняване на нарушението и в/ да наложи административно наказание.

Административните наказания, които могат да бъдат наложени по Регламент (ЕС) 2016/679 от компетентните органи, съгласно чл. 82 от Регламент (ЕС) 2016/679 са два вида: имуществена санкция или глоба. Видът и размерът на наказанието зависи от това дали администраторът е юридическо или физическо лице и какво е извършеното нарушение. Безспорно установена в практиката на административните съдилища в страната е възможността, предвидените административни наказания, да бъдат налагани както в рамките на производство по реда на ЗАНН (в случаите по чл. 12 ЗЗЛД), така и по реда на АПК (в случаите когато КЗЛД действа като колективен административен орган, чиито актове - решения, се обжалват по реда на АПК).

Следователно, като е обективирала в решение правомощието си за налагане на наказание за извършено нарушение на чл. 5, § 2, чл. 32, чл. 32, § 1, буква „г“ и чл. 32, § 4 от Регламент (ЕС) 2016/679, КЗЛД е упражнила законосъобразно нормативно установените си функции, свързани с контрола по спазването на Регламент (ЕС) 2016/679. Предвид изложеното, доводите на оспорващия, че е следвало да се образува административнонаказателно производство по реда на ЗАНН, са неоснователни.

Изложеното обосновава извод, че в хода на адаминистративното производство не са допуснати нарушения на административно производствените правила, които да бъдат квалифицирани като съществени по смисъла на чл. 146, т. 3 от АПК и да обуславят отмяната му.

Оспореното решение е постановено и в съответствие с приложимите материалноправни разпоредби, при което наведените в противен смисъл доводи от оспорващия се явяват неоснователни.

В разпоредбата на чл. 4, т. 7 от Регламент 2016/679 се определя, че администратор на лични данни е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с друг определя целите и средствата за обработване на лични данни, когато

целите и средствата за това обработване се определя от правото на съюза или правото на държавата членка. В т. 8 от Регламента е записана и дефиницията на „обработващ лични данни“, а именно: „физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора“. В този смисъл, за да носи отговорност едно лице за обработване на личните данни на друго лице в нарушение на ЗЗЛД и Регламент 2016/679, то лицето използващо неправомерно данните следва да има качеството „администратор“ или „обработващ лични данни“. По делото не се спори, че ПОД „ТОПЛИНА“ АД е администратор на лични данни

Съгласно легалното определение на чл. 4, ал. 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.

Според заложеното в чл. 5 от Регламент 2016/679, личните данни следва да се обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“); да се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите“); да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“); да са точни и при необходимост да бъдат поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“); да са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, при условие че бъдат приложени

подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“); да са обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

Принципът за отчетност, регламентиран от чл. 5, § 2 от ОРЗД гласи, че администраторът на лични данни носи отговорност и следва да е в състояние - във всеки момент, да докаже - при обработване личните данни на физическото лице, спазване на принципите, закрепени в чл. 5, § 1 от регламента.

Съгласно разпоредбата на чл. 32, § 1 от Регламент (ЕС) 2016/679, 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: „а“ псевдонимизация и криптиране на личните данни; „б“ способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване; „в“ способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент; „г“ процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки е оглед да се гарантира сигурността на обработването. В § 2 на цитираната норма, 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. Според чл. 32, § 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.

Разпоредбата на чл. 24 от Регламента въвежда като задължение и

отговоронст на администратора на лични данни да въведе подходящите технически и организационни мерки, отчитайки факторите изброени в същия член. В тази връзка администраторът следва да оцени рисковете, свързани с конкретното обработване и да предприеме мерки за ограничаване на тези рискове. Мерките следва да гарантират подходящо ниво на сигурност, вкл. поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени. С оглед наличните по делото доказателства обоснован и законосъобразен е изводът на административния орган, че ПОД „Топлина“АД не е предприела необходимите организационни и технически мерки, за да защити личните данни на клиентите си. Самият факт, че е осъществен неоторизиран достъп до личните данни на клиентите на пенсионноосигурителното дружество, като тези данни са извлечени от трета неидентифицирана страна, независимо по какъв начин, обосновава извод за липсата на предприети технически и организационни мерки до степен създаваща необходимата гаранция за защитата им от неоторизиран достъп.

В чл. 25 от Регламент (ЕС) 2016/679 е залегнало задължение за администратора на лични данни, което се отнася до защитата на личните данни на етапа на проектиране и по подразбиране. В § 1 на цитираната разпоредба е посочено, че като взема предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, например псевдонимизация, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване, за да се спазят изискванията на настоящия регламент и да се осигури защита на правата на субектите на данни. А в § 2 е разписано, че администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, периода на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице

личните данни не са достъпни за неограничен брой физически лица.
В процесния случай, КЗЛД е достигнала до правилен извод, че администраторът не е предприел технически и организационни мерки, които да гарантират подходящо ниво на сигурност на личните данни, предоставени от клиенти на администратора. Дружеството е следвало да приложи мерки, които отговарят по-специално на принципите за защита на данните на етапа на проектирането и по подразбиране. Когато определя кои мерки са подходящи, администраторът следва да оцени съвременните технически и технологични достижения в съвкупност с разходите за прилагане, естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица. След извършване на такава оценка и анализ е следвало да приложи подходящи технически и организационни мерки за осигуряване на съобразено с конкретните рискове ниво на сигурност. Именно с тези си действия, дружеството е нарушило залегналото задължение, визирано в нормата на чл. 25 от Регламент (ЕС) 2016/679, както и задължението за въвеждането на подходящи технически и организационни мерки, съгласно чл. 32, § 1 от Регламент (ЕС) 2016/679, условия, гарантиращи съответствие с принципа за цялостност и поверителност, разписани в чл. 5, § 1, буква „е“ от Регламент (ЕС) 2016/679. В настоящият случай администраторът на лични данни е разбрал за нарушаване на сигурността на обработваните от него лични данни едва след като е получил заплашителен имейл от лицата достъпили информационната система на стария сайт на дружеството, което означава, че заложените информационни системи и инструменти за сигурност не са сработили по време на извършения неоторизиран достъп. Това, от своя страна обосновава категоричен извод, че липсват информационни механизми, които да гарантират невъзможност за неотризиран достъп до базата данни на дружеството.

Настоящият съдебен състав намира, че в случая е неприложима хипотезата на освобождаване от отговорност на администратор или обработващ лични данни съгласно чл. 83, § 2 и ал. 3 от ОРДЗ, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.Тежестта да докаже, че са взети подходящите организационни и технически мерки, е на администратора/ обработващия. Администраторът/обработващият следва да установи по несъмнен начин, че е предприел подходящите и ефективни организационни и технически мерки, така че по никакъв начин не е отговорен за изтичането на личните данни, което в случая не е сторено.

В съображение 74 от ОРЗД е предвидено, че администраторът е

длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с този 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. А в съображение 146 от ОРЗД е предвидено, че администраторът или обработващият лични данни следва да бъде освободен от отговорност, ако докаже, че по никакъв начин не е отговорен за вредите.

В случая от страна на ПОД „Топлина“АД не са представени неоспорими доказателства, че е приложило подходящите технически и организационни мерки за осигуряване на съобразено с конкретните рискове ниво на сигурност спрямо стария сайт на дружеството.

В обобщение на изложеното, настоящият съдебен състав обосновава извод, че административният орган законосъобразно е приел, че оспорващото дружество е допуснало нарушение на основни принципи при обработването на личните данни, установени в чл. 5, ал. 1, б. „е“, във връзка с чл. 32, § 1, буква „б“ и буква „г“, както и на чл. 24, § 1 и чл. 25 от Регламент /ЕС/ 2016/679.

Комисията разполага с оперативна самостоятелност, като в съответствие с предоставените й 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 конкретните физически лица – субекти 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. Административното наказание "глоба" или "имуществена санкция", предвидено в б. "и" на чл. 58, §2 има санкционен характер и се прилага в допълнение към мерките по б. "а" – б. "з" и б. "й" *или вместо тях*. 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 процесния случай, в условията на предоставената й оперативна

самостоятелност, КЗЛД е приела да приложи корективната мярка по чл.58, § 2, б. „и“ от Регламент /ЕС/ 2016/679 - „имуществена санкция“, заедно с такава по чл. 58, § 2, б. „г“.

Общите условия за налагане на административни наказания „глоба“ или „имуществена санкция“ са регламентирани в чл.83 от Регламент /ЕС/ 2016/679. В §2 на чл.83 е предвидено, че при вземане на решение дали да бъде наложено административно наказание „глоба“ или „имуществена санкция“ и при определяне на техния размер, във всеки конкретен случай надлежно се разглеждат елементите, изчерпателно посочени в б., б. „а“ – „к“. В случая Комисията е изложила ясни мотиви относно това кои обстоятелства възприема като отегчаващи отговорността и причините за това. Видно от характера на засегнатите обществени отношения и предвидените санкции, законодателят е презумирал високата обществена опасност на тези деяния. По делото не са установени факти, които да сочат по-ниска степен на обществена опасност от типичната за този вид нарушения, поради което и същото не може да се квалифицира като маловажно. Съдът приема, че размерът на санкцията е съразмерен с тежестта и продължителността на нарушението и е определен в съответствие с принципите установени чл.83, §1 от Регламент /ЕС/ 2016/679.

С оглед на изложеното жалбата на ПОД „Топлина“ следва да бъде отхвърлена като неоснователна.

При този изход на спора и на основание чл. 143, ал. 3 от АПК на ответника се дължат разноски за юрисконсултско възнаграждение в размер определен на основание чл. 24 от Наредбата за заплащане на правната помощ.

Предвид изложеното и на основание чл. 172, ал. 2 от АПК, Административен съд София- град, Второ отделение, 56-ти състав

Р Е Ш И:

ОТХВЪРЛЯ жалбата на Пенсионноосигурително дружество “ТОПЛИНА“АД, ЕИК[ЕИК], представлявано от Г. П. Л. и С. Т. Г. чрез пълномощник адв. К. Д. против решение № ПАИКД-13-7/23 от 28.02.2024 г. на Комисията за защита на личните данни в частта му, с която на основание чл. 58, §2, б. „и“ от Регламент (ЕС)2016/679 на дружеството е наложено административно наказание - имуществена санкция в размер на 20 000 лева, съгласно чл. 83, §4, б. „а“ за нарушение на чл. 24, ал. 1, чл. 25, ал. 1, чл. 32, § 1, б. „б“ и б. „г“ от Регламент (ЕС) 2016/679 и чл. 83, §

5, б. „а“ за нарушение на чл. 5, § 1, б. „е“ от Регламент (ЕС) 2016/679.
ОСЪЖДА Пенсионноосигурително дружество “ТОПЛИНА“АД, ЕИК[ЕИК], представлявано от Г. П. Л. и С. Т. Г. да заплати на Комисията за защита на личните данни разноски по делото в размер на 100 (сто) лева.
Решението подлежи на обжалване в 14-дневен срок от съобщаването му пред Върховния административен съд.

СЪДИЯ: