Р Е Ш Е Н И Е
№ 15329

гр. София, 07.05.2025 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 38 състав,** в публично заседание на 17.03.2025 г. в следния състав:

СЪДИЯ: Татяна Жилова

при участието на секретаря Елена Георгиева, като разгледа дело номер **7698** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

Съдебното производство е по реда на чл.145 - чл.178 Административнопроцесуалния кодекс (АПК) във връзка със Закона за защита на личните данни (ЗЗЛД) и Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните).

Образувано е по жалба на „Застрахователно акционерно дружество ДаллБогг: Живот и Здраве“ АД, ЕИК[ЕИК], със седалище и адрес на управление в [населено място], подадена от пълномощниците юрисконсулт Б. М. и адвокат Н. Л., срещу Решение № ПАИКД-13-17/2023 от 24.06.20221г. на Комисията за защита на личните данни (КЗЛД).

С оспорения административен акт КЗЛД е наложила на жалбоподателя административно наказание имуществена санкция в размер на 50 000 лева съгласно чл.83, §4, буква „а“ от Регламент (ЕС) 2016/679 (ОРЗД) за нарушение на чл.25, ал.1 и чл. 32, §1, буква „б“ от същия регламент.

Жалбоподателят Застрахователно акционерно дружество ДаллБогг:Живот и Здраве“ АД, чрез процесуалните си представители, юрисконсулт Б. М. и адвокат Н. Л., оспорва решението като незаконосъобразен по всички основания по чл.146 от АПК. Твърди, че не извършил вмененото му нарушение, тъй като е взел всички необходими и подходящи мерки за гарантиране сигурността на обработването на личните данни на застрахованите лица. Сочи, че наздзорните органи не са утвърдили минимален стандарт за информационна и киберсигурност, който да е задължителен за застрахователните дружества. Счита, че административното производство неправилно е проведено по реда на чл.38 от ЗЗЛД, който е приложим за разглеждане на жалби от пострадали лица, каквито няма подадени. В случая жалбоподателят сам е уведомил КЗЛД по реда на чл.33 от ОРЗД за извършена кибератака и пробив в сигурността на обработваните лични данни, което

предполага друг ред за провеждане на производството. Във връзка с това, счита, че е приложим общият ред по ЗАНН за налагане на административно наказание. Отделно от това, твърди, че действията на КЗЛД не са в съответствие с целта на закона за гарантира защитата на личните данни, тъй като тя като надзорен орган на може да приложи други мерки в рамките на нейната компетентност, вместо да налага административно наказание, с което целта на закона не се постига. Поради това се иска отмяна на административния акт. Заявява претенция за разноски.
Ответникът – Комисията за защита на личните данни, чрез процесуалните си представители юрисконсулт А. Я. и юрисконсулт Л. М., в представено писмено становище оспорва жалбата. Поддържа и доразвива мотивите на административния акт. Твърди, че жалбоподателят не е въвел системи, които да отговарят на изискванията за защита на личните данни съгласно международен стандарт ISO 27701. Претендира юрисконсултско възнаграждение.
СЪДЪТ, като прецени, че административният акт подлежи на оспорване и жалбата е подадена от неговия адресат в законовия срок, намира същата за процесуално допустима.
Разгледана по същество, жалбата е неоснователна.
Установени факти:
Всички относими факти се установяват от административната преписка и заключението на съдебно-техническата компютърна експертиза, което не е оспорено от страните и се цени от съда като компетентно, добросъвестно и обективно.
Производството пред КЗЛД е образувано във връзка с Уведомление по чл.33 от ОРЗД за нарушение на сигурността на данните с вх.№ПАИКД-13-17 от 31.03.2023г., подадено от жалбоподателя. В уведомлението се съобщава за получен заплашителен имейл от хакер, който е проникнал в системите на дружеството и в продължение на 6 месеца е събирал лични данни на застрахованите лица и данни за застрахователните полици. Предполагаемо са достъпени снимки на шофьорски книжки, които са копирани пир сключване на договорите за застраховка. Съобщава се , че може да бъдат засегнати данни за 250 000 лица.
В 72-часовия период след установяване на инцидента жалбоподателят е уведомил субектите на лични данни чрез обща публикация на интернет страницата си.
След получаване на уведомлението КЗЛД е извършила оценка на риска и е приела наличие на „високо ниво на риск“, поради което председателят на КЗЛД е разпоредил извършване на проверка на място. С оглед на проверката са изискани документи, от които да се установят предприетите технически и организационни мерки относно физическата, персоналната и документалната защита на личните данни, защитата на автоматизираните информационни системи и/или мрежи и криптографска защита – представени от жалбоподателя по опис.
Проверката е извършена в административната сграда на жалбоподателя на 21.03.2024г., а констатациите са отразени в двустранно подписан протокол, който не е приложен към административната преписка, но доколкото неговото съдържание е възпроизведено в административния акт и не се оспорва от жалбоподателя, съдът приема, че той е редовно съставен.
Безспорно е между страните, че в резултат на неоторизирания достъп са засегнати две системи на застрахователя: 1) У. приложение, съдържащо издадените вече застрахователни полици, включващи три имена и ЕГН на застрахованите лица, а в част от случаите и имейл и телефонен номер за контакт; и 2) М. сървър, чрез който е прихваната кореспонденцията с отдел „Автомобилна ликвидация“, където са налични данни за заведените автомобилни щети, данни от регистрационните талони на автомобилите, данни от свидетелствата за самоуправление на водачите и банковите им сметки.
Както към момента на проверката на място, така и към момента на приключване на

административното производство пред КЗЛД жалбоподателят не е бил в състояние да установи категорично броя на засегнатите физически лица и обема на разкритите данни.
Нерегламентираният достъп е осъществен чрез компютърен вирус или фишинг атака, с цел откradване на потребителски имена и пароли. Установени са изтекли потребителски имена и пароли поне на двама служители от двете системи. Съдебната експертиза потвърждава, че информационната система на дружеството е приела неоторизирания достъп като „приятелски вход“, поради което е предоставяла данни в продължителен период от време без да разпознае пробива.
Според заключението на съдебната експертиза, дружеството е предприело необходимите мерки в съответствие с международния стандарт за управление на информационната сигурност ISO 27001. Работните станции са били защитени със сложни пароли, изискващи смяна на всеки 180 дни, антивирусната програма е с централна конзола за управление, инсталирани са срочни актуализации на сигурността. Сървърите са имали ежедневни архиви (бекъп) на два различни физически адреса в [населено място] и в [населено място], което позволява възстановяване на цялата база данни при срив. Вещото лице дава заключение, че към момента на пробива информационната система на жалбоподателя е била добре защитена на ниво мрежова сигурност. По отношение на киберсигурността винаги може да се предприемат допълнителни мерки, както например двуфакторната автентификация при достъпване на системата, каквото жалбоподателят започва да въвежда след инцидента.
Както в административното, така и в съдебното производство жалбоподателят не представя доказателства да е сертифициран съобразно международен стандарт за защита на личните данни ISO 27701 или да е въвел мерките в него, няма наведени и такива твърдения.
КЗЛД е изложила подробни мотиви относно размера на имуществената санкция. Като е съобразила годишния финансов оборот на дружеството за предходната 2022г. в размер на 206 422 933 лева, КЗЛД е определила санкция в размер на 0.12% от годишния оборот.
Правни изводи:
В изпълнение на правомощията си по чл.168, ал.1 от АПК съдът извършва пълна проверка за законосъобразност на административния акт на всички основания по чл.146 от АПК, като не е ограничен от основанията, посочени от оспорващия.
1. Решението е постановено от КЗЛД в рамките на нейната компетентност по чл.63 Правилника за дейността на КЗЛД и на нейната администрация (Правилника). Оспореният административен акт е издаден от компетентен орган в законен състав и с мнозинство съгласно чл. 9, ал.3 от ЗЗЛД.
2. Решението е издадено в предвидената от закона форма, съгласно чл. 59 АПК, като съдържа необходимите посочени в ал. 2 реквизити.
3. При издаване на оспорения административен акт не са допуснати съществени административно-процесуални нарушения.
КЗЛД като надзорен орган със специална компетентност разполага с правомощията по чл.58 от ОРЗД във всички случаи, не само когато е сезирана със жалба от засегнати субекти на лични данни. Подаването на уведомление по чл.33 от ОРЗД е в изпълнение на задължение на администратора на лични данни, но то по никакъв начин не ограничава правомощията на комисията, която дължи пълна проверка на всички обстоятелства в хода на образуваното административно производство. При установено нарушение при обработването на лични данни, обект на защита е не само всеки засегнат субект на лични данни, но и обществените отношения по защита на личните данни като цяло.
Възраженията на жалбоподателя за неприложимост на производството по чл.38 от ЗЗЛД са неотносими. Административното производство е проведено по реда на чл.63 от Правилника,

който урежда действията на КЗЛД при подадено уведомление по чл.33 от ОРЗД. Съгласно чл.63, ал.3 от Правилника, след приключване на проверката по ал.1 или 2 комисията постановява решение, като може да приложи мерките по чл.58, параграф2, букви “а” – “з” и “й” от Регламент (ЕС) 2016/679 или по чл.80, ал.1, т. 3, 4 и 5 от ЗЗЛД и в допълнение към тези мерки или вместо тях да наложи административно наказание в съответствие с чл.83 от Регламент (ЕС) 2016/679, както и по глава девета от ЗЗЛД.
В случая КЗЛД е упражнила правомощията си по реда на Правилника в съответствие с принципа за служебното начало, утвърден в чл.9, ал.2 от АПК – административният орган събира всички доказателства и когато няма искане от заинтересованата страна, и в съответствие с принципа за истинност, утвърден в чл.7, ал.1 и ал.2 от АПК - административните актове се основават на действителните факти от значение за случая, като на преценка подлежат всички факти и доводи от значение за случая.
Редът и условията за налагане на административно наказание по ОРЗД и ЗЗЛД са специални по отношение на ЗАНН и съответно дерогират приложението на последния.
4. Оспореният административен акт е постановен в съответствие с материалноправните разпоредби на закона.
Съгласно чл.25, §2 от ОРЗД администраторът на лични данни е длъжен да въведе както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки. Кои мерки са подходящи, се определя като се вземат 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.
Подходящи мерки за сигурността на обработването са посочени, inter alia, в чл.32, §1 от ОРЗД: 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 с оглед да се гарантира сигурността на обработването.
Както се установи в производството, жалбоподателят е предприел в достатъчна степен само част от мерките по буква „в“, извършвайки ежедневен бекъп на данните на два различни физически сървъра, както и мерки за гарантиране на цялостност, наличност и устойчивост на системите и услугите за обработване съгласно буква „в“.
Не са предприети обаче подходящи мерки за поверителност на данните и защита от външна намеса, не са въведени механизми за оценка на рисковете и на ефективността на защитата, каквито технически възможности са налице чрез двуфакторна идентификация на потребителите. Не са необходими специални технически познания, за да се разбере, че смяна на паролите на служителите на всеки 180 дни е най-минималното ниво на защита. Задължение на администратора на лични данни е да има проактивно поведение и сам да следи за развитието и състоянието на техниката, като полага дължимата грижа да въвежда тези мерки, които отговарят на новите и актуални стандарти за безопасност.
В областта на защитата на личните данни Българският институт за стандартизация е въвел стандарт БДС EN ISO/IEC 27701:2021 (достъпен на официалната интернет страница на БИС https://bds-bg.org/bg/project/show/bds:proj:112561), който надгражда стандартите ISO/IEC 27001 и ISO/IEC 27002 за управление на неприкосновеността на информацията и се прилага заедно с тях. Макар и да липсва изрична законова разпоредба, която да задължава администраторите на лични

данни да бъдат сертифицирани по станарт ISO/IEC 27001 и ISO/IEC 27002, стандартите представляват добра практика за защита на личните данни, която би следвало да се познава от жалбоподателя и той да приведе обработването в съответствие с нея, за да отговори на общото изискване на чл.25, §1 от ОРЗД. Не се установи към момента на неоторизирания достъп до личните данни жалбоподателят да е отговарял на завишените изисквания на стандарт БДС EN ISO/IEC 27701:2021. Допускайки занижено ниво на сигурност на достъпа до информационните системи, жалбоподателят е нарушил изискванията на чл.25, §1 и чл.32, §1 от ОРЗД.
Наложената имуществена санкция е в границите, определени в чл.83, §4 от ОРЗД - в размер до 10 000 000 EUR или, в случай на предприятие — до 2 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока. Наложената санкция е справедлива. За да породи необходимия възпиращ ефект, тя е съобразена с имущественото състояние на жалбоподателя от една страна, от друга страна подаването на уведомление по чл.33 от ОРЗД е преценено като смекчаващо обстоятелство. Правилно КЗЛД е определила имуществена санкция, клоняща към минималния размер, която в случая отговаря на изискванията на чл.83, §1 от ОРЗД за ефективност и пропорционалност.
5. Оспореното решение е в съответствие с целите на ОРЗД и ЗЗЛД да гарантират защита на физическите лица от неправомерно обработване на данните им.
Обстоятелството, че администраторът на лични данни е предприел действия за повишаване на сигурността на личните данни веднага след пробива в системите му, не обосновава отмяната на административния акт, тъй като няма отношение към преценката за законосъобразността му.
Не са налице отменителни основания по чл.146 от АПК, поради което жалбата срещу административния акт се отхвърля.
Разноски:
При този изход на правния спор разноските са в тежест на жалбоподателя. На основание чл.143, ал.3 от АПК жалбоподателят следва да заплати на ответника юрисконсултско възнаграждение в размер на 100 лева, определен съгласно чл. 24 от Наредбата за заплащането на правната помощ във връзка с чл. 37, ал.1 от Закона за правната помощ.
Така мотивиран и на основание чл.172, ал.2, Административен съд София-град, 38 състав,
Р Е Ш И :
ОТХВЪРЛЯ жалбата на „Застрахователно акционерно дружество ДаллБогг: Живот и Здраве“ АД срещу Решение № ПАИКД-13-17/2023 от 24.06.20221г. на Комисията за защита на личните данни.
ОСЪЖДА „Застрахователно акционерно дружество ДаллБогг: Живот и Здраве“ АД да заплати на Комисията за защита на личните данни разноски в размер на 100 (сто) лева.
Решението подлежи на обжалване пред Върховния административен съд с касационна жалба, подадена чрез АССГ в 14-дневен срок от съобщаването му.

Съдия: