Р Е Ш Е Н И Е
№ 24508

гр. София, 22.11.2024 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 22 състав,** в публично заседание на 25.10.2024 г. в следния състав:

СЪДИЯ: Десислава Корнезова

при участието на секретаря Илияна Тодорова, като разгледа дело номер **8054** по описа за **2024** 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/.

Образувано е по жалба на Агенция по заетостта, представлявана от изпълнителния директор С. В., срещу решение № ПАИКД -13-2/2024 г. от 24.07.2024 г. на Комисията за защита на личните данни /КЗЛД/.

В жалбата се твърди, че решението е издадено в противоречие с материалноправните разпоредби и съществено нарушение на административнопроизводствените правила. Не се оспорва, че на 22.01.2023 г. е извършена кибер - атака срещу сървърите на Агенция по заетостта, като се посочва, че длъжностните лица са уведомили изпълнителния директор П. М., както и че КЗЛД е била уведомена за тази кибер-атака едва през 2024г. Твърди се, че неправилно е приложен материалният закон като е ангажирана отговорността на Агенция по заетостта, а не на представляващата я към този момент П. М.. От края на 2023 г. са били предприети редица действия за защита на обработваните и съхранявани от Агенция по заетостта лични данни. Навеждат се доводи, че предвид възприетото в мотивите на оспореното решение, че нарушението е извършено по небрежност, то отговорен е изпълнителният директор към момента на неговото извършване. Ето защо, решението било прието в нарушение на процесуалните правила без легитимираното лице да е уведомено за производството и да е взело участие в него. Прави се извод, че неправилно бил определен и размерът на наказанието.

В проведеното открито съдебно заседание, жалбоподателят се представлява от юрк. Е.

М., която поддържа жалбата. Моли за отмяна на атакуваното решение и присъждане на извършените по делото разноски. Съображенията за основателността на жалбата са обобщени в представените писмени бележки.
Ответникът – Комисията за защита на личните данни, чрез процесуалния си представител юрк. М. И.- К., в писмено становище от 04.10.2024 г. оспорва жалбата и моли решението да бъде оставено в сила. Посочва, че производството във връзка с уведомления по чл. 33 от Регламент (ЕС) 2017/679 е особено производство, което има за цел да се установи какви мерки са взети от администратора на лични данни преди инцидента, за да се предотврати той, както и да се удостоверят предприетите мерки за намаляване на вредните последици и на повторното настъпване на подобен инцидент. Страна в това производство бил администраторът на лични данни, който по смисъла на чл. 4, § 7 от Регламента, можел да бъде както физическо, така и юридическо лице. Акцентира, че в случая безспорно администраторът е Агенция по заетостта. Позовава се и на чл. 83 от Регламента, в който вида наказание се определял в зависимост от това дали санкционираното лице е физическо или юридическо лице. Твърди, че правилно е проведена процедурата по установяване на нарушенията и е определен видът и размерът на наложените наказания.
В проведеното заседание на 25.10.2024г. ответната страна се представлява от старши експерт А. Я., който оспорва жалбата. Моли съдът да я отхвърли, като неоснователна и недоказана и да потвърди оспорвания административен акт. Претендира се присъждане на юрисконсултско възнаграждение.
Софийска градска прокуратура – редовно призована не взема участие в производството.
Административен съд София-град, като обсъди релевираните с жалбата доводи и прецени събраните по делото доказателства по реда на чл. 235, ал. 2 ГПК във вр.чл. 144 АПК, приема за установено следното от фактическа страна:
Административното производство е било образувано по повод постъпило уведомление /сигнал/ с вх. № ПАИКД-13-2#2/04.01.2024г. от Агенция по заетостта до КЗЛД за нарушение на сигурността на данните по чл. 33 от Регламент (ЕС) 2017/679.
Изпратено е писмо от КЗЛД с изх. № ПАИКД-13-2#1/18.01.2024г. до Агенция по заетостта, с което е изискана допълнителна информация за изясняване на фактите и обстоятелствата във връзка с получения сигнал.
Постъпил е отговор от Агенция по заетостта с вх. № ПАИКД-13-2#2/25.01.2024г. във връзка с направеното запитване.
Изпратено е писмо от КЗЛД с изх. № ПАИКД-13-2#3/02.02.2024 г. до Министерство на електронното управление, ИА „Инфраструктура на електронното управление“, Главна дирекция „Борба с организираната престъпност“, Държавна агенция „Национална сигурност“ със запитване за предоставяне на информация във връзка с възникналата на 22.01.2023 г. кибер атака срещу сървърите на Агенция по заетостта.
Депозиран е отговор на Министерство на електронното управление с вх. № ПАИКД -13-2#4/09.02.2024г. с приложения до КЗЛД.
Изпратен е отговор на Министерство на електронното управление с вх. № ПАИКД-13-2#5/13.02.2024г. с приложени към него писмо с анализ по случая и доклад на служител по мрежова и информационна сигурност.
От Агенция по заетостта с вх. № ПАИКД-13-2#6/15.03.2024г. е била представена допълнителна информация към уведомление за инцидент № 13906 от 22.01.2023г.
Последвало е изпращането на ново писмо от КЗЛД до Агенция по заетостта с изх. №

ПАИКД-13-2#9/22.03.2024г., като са постъпили от жалбоподателя отговори вх. № ПАИКД-13-2#11/28.03.2024г. и вх. № ПАИКД -13-2#12/12.04.2024г. с предоставена информация.

КЗЛД с уведомление изх. № ПАИКД-13-2#15/16.05.2024г. е изискала извършване на допълнителна проверка във връзка с кибер атаката срещу сървърите на Агенция по заетостта, във връзка с което е поискана допълнителна информация и е изпратен въпросник за проверка на администратор на лични данни.

Изпратени са били отговори от Агенция по заетостта с вх. № ПАИКД -13-2#16/04.06.2024г. с предоставена информация и документи, както и с вх. № ПАИКД -13-2#17/13.06.2024г. с отговори на общ въпросник.

Проведено е било заседание на КЗЛД, на което присъстват членовете В. К., М. М., Ц. Ц., В. Ц. и служител от администрацията на КЗЛД. Изслушан е доклад на Дирекция „Правно – аналитична информационна и контролна дейност“, констативен акт от проверка по документи.

Административното производство е приключило с приемането на решение № ПАИКД-13-2/2024г. от 24.07.2024г. на Комисията за защита на личните данни. Решението е изпратено с придружително писмо изх. № ПАИКД -13-2#20/24.07.2024г.

Подадена е жалба на Агенция по заетостта с рег. № ПАИКД -13-2#21/08.08.2024г.

По делото е представена заповед № РД-11-00-638/17.01.2024г. на Агенция по заетостта за създаване на работна трупа във връзка с дейностите по обработване на лични данни, заповед № РД-11-00-2114/25.04.2024г. за определяне на екип, извършващ оценка на въздействието на личните данни, заповед № РД-11-2822/25.09.2023 г. на изпълнителния директор на Агенция по заетостта за създаване на работна група във връзка с дейността по обработване на лични данни; протокол за оценка на въздействие на характера на обработваните лични данни; доклад с вх. №30-00-30529/31.08.2023г. от Р. Д., служител от мрежова и информационна сигурност относно предприети действия за възникнал кибер инцидент на 21.01.2023г., доклад вх. № 274/27.01.2023г. за текущо състояние на виртуален частен облак на АЗ, след регистриран инцидент – криптиране на файлове, изготвен от „Дария Ентърпрайсиз“ ЕООД, план от 23.01.2023г. за реакция на възникнал кибер- инцидент на 22.01.2023 г., утвърден от изпълнителния директор на АЗ, актуализиран план от 09.02.2023г. за реакция на възникнал кибер- инцидент на 22.01.2023 г.; представени са и сигнали до ГДБОП – МВР.

При така установените факти, Административен съд София-град достигна до следните правни изводи:

Жалбата е процесуално допустима, защото е подадена срещу подлежащ на оспорване пред съд административен акт, който неблагоприятно засяга правната сфера на Агенция по заетостта, с оглед което е налице правен интерес от обжалването. Предвид липсата на доказателства относно точната дата, на която решението на Комисията за защита на личните данни е съобщено на жалбоподателя, съдът приема, че е спазен преклузивният 14-дневен срок за оспорване.

Разгледана по същество, жалбата е НЕОСНОВАТЕЛНА.

На първо място, Комисията за защита на личните данни по силата на чл. 6, ал.1 от ЗЗЛД е постоянно действащ независим надзорен 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 Регламент (ЕС) 2016/679 и на този закон. Председателят и членовете на КЗЛД са избрани с решение на НС, обн.

ДВ, бр. 35 от 22.04.2014 г., като Ц. Н. С. е освободен с решение на НС, обн. ДВ, бр. 92 от 22.11.2019г. Правомощията на Комисията са предоставени с разпоредбата на чл. 58, § 2, б. „и“ от Регламент (ЕС) 2016/679, съгласно която разпоредба всеки надзорен орган има корективните правомощия да налага административно наказание „глоба“ или „имуществена санкция“ съгласно член 83, в допълнение към мерките, посочени в настоящия параграф, или вместо тях, в зависимост от особеностите на всеки отделен случай. Доколкото Комисията е сезирана по чл. 33 от Регламент (ЕС) 2016/679, то в нейните правомощия е да се произнесе с решение, което подлежи на оспорване пред административния съд. В чл. 33 от Регламента е предвидено задължението на администратора на лични данни при случай на нарушение на сигурността на личните данни, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява 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. В случая на основание чл. 55 от Регламента, КЗЛД се явява органа териториално компетентен да изпълнява задачите и да упражнява правомощията в Република България.

Съгласно чл. 8, ал. 6 и ал. 7 от Правилника за дейността на Комисията за защита на личните данни и на нейната администрация заседанията на Комисията се провеждат, ако на тях присъстват най-малко трима от членовете на нейния състав. На основание чл. 9, ал. 3 от ЗЗЛД решенията на Комисията се вземат с мнозинство от общия брой на членовете й. На проведеното на 17.07.2024 г. заседание на КЗЛД, когато е взето оспореното решение, са присъствали четирима от членовете на Комисията. Решението е прието с единодушие на присъстващите, което е достатъчно по закон.

Предвид горното и независимо, че е изтекъл мандатът на председателя и на членовете на КЗЛД, по аргумент от чл. 7, ал. 2 ЗЗЛД съдът счита, че актът е постановен от компетентен орган и не е налице основанието по чл. 146, т. 1 АПК за прогласяване на нищожността му.

На второ място, атакуваното решение е издадено в писмена форма, мотивирано е, изложени са подробно фактическите основания и същите са подведени под относимата правна квалификация /чл. 59, ал. 2 АПК/. Волята на административния орган е ясно изразена, не съществуват пропуски или грешки, което е предпоставка за правилното упражняване на съдебния контрол за законосъобразност и осигурява възможност на оспорващия да организира адекватно защитата си във висящия съдебен процес. Не се констатираха несъответствия или противоречия между мотивите и разпоредителната част на решението. Не е налице основание за отмяна на акта по чл. 168, ал. 1 във връзка с чл. 146, т. 2 АПК.

На трето място, липсват данни за допуснати в хода на административното производство процесуални нарушения, които съществено да са ограничили правото на защита на засегнатото лице или ако не бяха допуснати, органът да би постановил акт в противен смисъл. Осигурено е правото на жалбоподателя да участва в производството, да представи доказателства и да формулира своите доказателствени искания, изискана е информация и от други административни органи, която е обсъдена при установяване на относимите факти. Не е налице основание за отмяна на акта по чл. 168, ал. 1 във връзка с чл. 146, т. 3 АПК.

На четвърто място, административният акт е издаден при правилно приложение на материалния закон - чл. 146, т. 4 АПК.

Легалната дефиниция на понятието „лични данни“ се съдържа в чл. 4, § 1, от

Регламент (ЕС) 2016/679, това е всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице. Според чл. 4, § 2 от Регламент (ЕС) 2016/679 „обработване“ на лични данни е 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.

В разпоредбата на чл. 4, § 7 от Регламент (ЕС) 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. По делото не е спорно, че Агенция по заетостта е администратор на лични данни. Не е спорно, а и от представените по делото доклади се установява, че на 22.01.2023 г. е извършена кибер атака срещу сървърите на Агенция по заетостта, следствие на която почти сто процента от компютрите са били засегнати от вирус, както и деловодната система, всички сървъри и виртуална среда са с криптирани файлове. Криптирани са били личните данни на 18 300 служители, 4731 кандидата за работа, 157 980 потребители, чиито лични данни се обработват и съхраняват в ИС „НБД“, както и личните данни на 56 000 чужди граждани, чиито данни, обработвани в регистър „Трудова миграция“ са загубени и невъзстановени. Категории данни на физически лица, засегнати от нарушението са: име, адрес, паспортни данни, месторождение, телефон, имейл, семейно положение, произход, образование, лични данни, които се отнасят до физическото и психическото здраве.

Спорът по делото е правен и се изразява в това дали оспорващият е осъществил състава на вменените му нарушения по чл. 33, § 1, чл. 32, §1, б. „б“ и §2, чл. 5, § 2 във връзка с чл. 33, § 5 от Регламент (ЕС) 2016/679.

В случай на нарушение на сигурността на личните данни за администратора възникват редица задължения по силата на Регламент (ЕС) 2016/679. Сред тях е и това по чл. 33, § 1 от Регламента, а именно: без ненужно забавяне и когато това е осъществимо- не по-късно от 72 часа след като е разбрал за нарушението да уведоми надзорния орган, 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. Безспорно установено в случая е, че такова уведомление съгласно горепосочените изисквания не е направено в срока от 72 часа. Жалбоподателят, чрез представляващия го изпълнителен директор, сам е установил това обстоятелство и е подал сигнал до КЗЛД в тази връзка. Административният орган е наложил наказание по чл. 58, § 2, буква „и“ от Регламент (ЕС) 2016/679- „имуществена санкция“. В административното производство, а и по делото не са

посочени обстоятелства за забавянето над 72 часа, нито са ангажирани доказателства в тази посока, въпреки изрично отправеното запитване от страна на КЗЛД в тази посока. Ето защо, правилно е ангажирана отговорността на Агенция по заетостта за нарушение на изискването по чл. 33, § 1 от Регламента за уведомяване на надзорния орган за нарушение на сигурността на личните данни.

Съдът намира за неоснователно възражението, че в случая санкционираното лице е следвало да бъде не администраторът на лични данни, а физическото лице, което го е представлявало към момента на извършване на нарушението. Видно от редакцията на чл. 33, § 1 от Регламент (ЕС) 2016/679, посоченото дължимо поведение е именно на администратора на лични данни. Съгласно разпоредбата на чл. 4, § 7 от Регламент (ЕС) 2016/679, администратори на лични данни могат да бъдат както физически, така и юридически субекти, следователно отговорност за неизпълнение на разписаните задължения могат да се носят и от юридически лица. По делото не се спори, че жалбоподателят Агенция по заетостта има качеството администратор на лични данни. Ето защо съдът приема, че правилно е ангажирана отговорността именно на административния орган. В подкрепа на това разбиране е и съдебната практика, например решение № 8668/07.10.2022г. по дело № 3441/2022 г. на ВАС.

На следващо място, администраторът на лични данни е санкциониран за за нарушение на чл. 32, § 1, буква „б“ и чл. 32, §2 от Регламент (ЕС) 2016/679 и чл. 83, §5, б. „а“ за нарушение на чл. 5, § 2 във връзка с чл. 33, § 5 от Регламент (ЕС) 2016/679.

Разпоредбата на чл. 32, § 1, буква „б“ гласи, че 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 способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване. В параграф 2 от същия член от Регламент (ЕС) 2016/679 се уточнява, че 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.

В свое решение № 8668/07.10.2022 г. по дело № 3441/2022 г. Върховният административен съд посочва, че „възприемането на тезата на Комисията, която се налага от процесното решение, че при осъществен неправомерен достъп до данните, винаги е налице нарушение на чл. 32, § 1 ОРЗД, означава да се приеме, че всеки който е станал обект на каквото и да е посегателство, следва да понесе отговорност, че е допуснал

осъществяването на същото, независимо че може да е взел всички възможни към този момент технически и организационни мерки за защита на данните. Именно за да не се допусне това, Комисията дължи изследване и преценка на съществуващите до нарушението мерки за защита на данните и преценка дали те са били подходящи и съобразени с 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“. Тоест за да се приеме, че е налице нарушение на чл. 32, § 1 и §2 от Регламента, е необходимо да се изследват и анализират мерките, които вече са били предприети за гарантиране защитата на личните данни към момента на осъществяване на посегателството върху лични данни, като се проучат и анализират техническите параметри и характеристики на съществуващите системи, както и какви организационни мерки за защита на данните са съществували и до каква степен те са били подходящи, „само по този начин, ще са гарантирани както правата на субекта на данните, така и правата на администраторите на лични данни. (решение № 8668/07.10.2022 г. по адм. дело № 3441/2022 г.).

Тук е мястото да се цитират и разясненията дадени в решение от 14.12.2023 г. на трети състав на СЕС по дело № С-340/2021 г., че чл. 24 и 32 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) трябва да се тълкуват в смисъл, че *„неразрешено разкриване на лични данни или неразрешен достъп до такива данни от „трета страна“ по смисъла на член 4, точка 10 от този регламент сами по себе си не са достатъчни, за да се приеме, че приложените от съответния администратор технически и организационни мерки не са „подходящи*“. Чл. 32 от Регламент 2016/679 трябва да се тълкува в смисъл, че *„преценката дали приложените от администратора технически и организационни мерки по този член са подходящи трябва да бъде направена от националните юрисдикции конкретно, като се вземат предвид рисковете, свързани със съответното обработване, и като се прецени дали естеството, обхватът и прилагането на тези мерки са съобразени с тези рискове“*. Принципът на отчетност на администратора, закрепен в чл. 5, § 2 и конкретизиран в чл. 24 от Регламент 2016/679, трябва да се тълкува в смисъл, че *„в исково производство за обезщетение, администраторът носи тежестта за*

доказване на обстоятелството, че приложените от него мерки за сигурност по чл. 32 са подходящи“. Следва да се има предвид и, че *„администраторът не се освобождава от задължението си по член 82, параграфи 1 и 2 за обезщетяване на претърпените от дадено лице вреди само поради факта че тези вреди произтичат от неразрешено разкриване на лични данни или неразрешен достъп до такива данни от „трета страна“ по смисъла на член 4, точка 10 от посочения регламент“*.

В мотивите на атакуваното решение КЗЛД посочва, че администраторът на лични данни е следвало да приеме подходящи технически и организационни мерки, отчитайки факторите по чл. 24 Регламента, като извърши и оценка на рисковете, свързани с обработването и да въведе мерки за ограничаване на тези рискове. Административният орган е приел, че се е изисквало проследяване на различните рискове, произтичащи от обработването на лични данни, включително случайно, неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предавани, съхранявани или обработвани по друг начин данни. В тази връзка Комисията е предприела действия за установяване изпълнил ли е жалбоподателят тези свои задължения. Следва да се отбележи, че в съображение 83 от Регламента се посочва, че с цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на настоящия регламент, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително 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. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, материални или нематериални вреди.

В случая подобен анализ на риска би показал уязвимостта на остарялата версия на Windows exchange server, както и липсата на устройство или друг механизъм за съхраняване на резервно копие от информацията в регистър „Трудова миграция“, която се получава по електронен път от Дирекция „Миграция“- МВР и обработването ѝ единствено в електронния архив на ДС „А.“ не се позволява последващото ѝ възстановяване.

Въпреки отправеното запитване от КЗЛД в административното производство и по делото липсват данни за изготвена оценка на риска за сигурността на данните преди възникването на инцидента. Обоснован се явява изводът на органа, че администраторът на лични данни не се е съобразил с принципите на защита на данните по подразбиране съобразно чл. 25 от Регламент (ЕС) 2016/679, съответно не е предприел необходимите технически и организационни мерки и е нарушил разпоредбите на чл. 32, § 1, буква „б“ и чл. 32, §2 от Регламент (ЕС) 2016/679.

Съдът споделя изводите на ответника и по отношение на наличието на предпоставките по чл.5, § 2 във връзка с чл. 33, § 5 от Регламент (ЕС) 2016/679. Съгласно разпоредбата на чл. 33, § 5 от Регламент (ЕС) 2016/679, администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган да провери дали е спазен настоящият член относно необходимите действия по уведомяване на надзорния орган за нарушение на сигурността на личните данни. На следващо място в чл. 5, § 2 от Регламент (ЕС) 2016/679 е възпроизведен принципът за отчетност, съгласно който администраторът носи отговорност и е в състояние да докаже изпълнението на останалите основните принципи за законосъобразност, добросъвестност и прозрачност; ограничение на целите; свеждане на данните до минимум; на точност; на ограничение на съхранението; цялостност и поверителност. Както е посочено в мотивите на оспореното решение, в случая принципът на отчетност се изразява в задължението на Агенция по заетостта да извърши документиране на фактите, свързани с нарушението на сигурността на личните данни, последиците от него и съответно предприетите действия. Тази документация дава възможност на надзорния орган да провери дали са спазени разпоредбите на чл. 33 от Регламент (ЕС) 2016/679, касаещи действията, които следва да се предприемат при констатиран пробив в сигурността на данните. С писмо рег. № ПАИКД – 13-2#9/22.03.2024г. КЗЛД е изискала допълнителна информация извършен ли е анализ на риска на правата и свободите на физическите лица към момента на възникване на нарушението. Отправено е искане и за представяна на доказателства относно изпълнението на задълженията по чл. 33, § 5 от Регламента относно документиране на нарушението, включително фактите, свързани с него, настъпилите последици и предприетите действия за справяне с нарушението. В своя отговор, Агенция по

заетостта посочва, че не са изпълнени задълженията по чл. 33 от Регламент (ЕС) 2016/679 да бъде информиран надзорния орган, както и че липсва документиране на нарушението на сигурността на личните данни, по реда на Регламент (ЕС) 2016/679. Представеният анализ на риска е от 2024 г., одитният доклад с рег. № 30-00-2470 е от 07.07.2023 г., т.е. половин година след извършване на нарушението, а доклад с вх. № 274/27.01.2023г. за текущото състояние на виртуален частен облак на Агенция по заетостта, касае техническото състояние на системите и не може да се възприеме като документиране на нарушението на сигурността на личните данни, по реда на приложимия Регламент. Същото важи и по отношение на изготвените план за реакция и актуализиран план за реакция с възникнал кибер инцидент на 22.01.2023г. Не на последно място, във връзка с направеното от жалбоподателя възражение, адресат на цитираните по- горе разпоредби е администраторът на лични данни и правилно е ангажирана именно неговата отговорност.

По изложените съображения, настоящият състав на съда споделя изводите на административния орган относно установено нарушение чл. 5, § 2 във връзка с чл. 33, § 5 от Регламент (ЕС) 2016/679.

За констатираните нарушения на основание чл. 58, параграф 2, буква „и“ от Регламент (ЕС) 2016/679 на Агенция по заетостта е било наложено наказание- имуществена санкция в общ размер 100 000 (сто хиляда) лева, както следва:

1) Съгласно чл. 83, § 4, буква „а“ -за нарушение на чл. 33, параграф 1 от Регламент (ЕС) 2016/679 - 25 000 (двадесет и пет хиляда) лева.

2) Съгласно чл. 83, § 4, буква „а“ -за нарушение на чл. 32, параграф 1, буква „б“ и чл. 32, параграф 2 от Регламент (ЕС) 2016/679 и чл. 83, § 5, буква „а“- за нарушение на чл. 5, § 2 във връзка с чл. 33, параграф 5 от Регламент (ЕС) 2016/679 - 75 000 (седемдесет и пет хиляда) лева.

Органът е обосновал защо налага имуществена санкция вместо някоя от другите предвидени мерки, а размерът на санкцията е обоснован с броя засегнати лица – 18 300 служители, 4 731 кандидати а работа, 157 980 потребители физически лица, гражданин на други държави – около 56 000 физически лица. Отчетен е фактът, че посредством изброените данни лицата могат да бъдат идентифицирани, което да доведе до загуба на контрол и поверителност на личните им данни, липсват доказателства относно смекчаване на предотвратяване на вредите относно засегнатите физически лица, не е проведено разследване, което да отговори има ли изтичане на лични данни и категоризиране на данните, сигналът е изпратен близо една година след извършване на нарушението.

Определената е формата на вината за двете нарушения. Като смекчаващи фактори са изтъкнати липсата на предишни нарушения, оказаното съдействие след сигнала. Съгласно разпоредбата на чл. 83, §2 от Регламента, когато се взема решение дали да бъде наложено административно наказание „глоба" или „имуществена санкция" и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат следните елементи: а.) естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда; б.) дали нарушението е извършено умишлено или по небрежност; в.) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни; г.) степента на отговорност на администратора или обработващия лични данни като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с членове 25 и 32; д.) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни; е.) степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него; ж.) категориите лични данни, засегнати от нарушението; з.) начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението; и.) когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, посочени в член 58, параграф 2, във връзка със същия предмет на обработването, дали посочените мерки са спазени; й.) придържането към одобрени кодекси на поведение съгласно член 40 или одобрени механизми за сертифициране съгласно член 42; к.) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението. В случая, КЗЛД е определила размера на санкцията като е изследвала и се е водила от всеки един от посочените в чл.83, §2 от Регламента критерии.

Предвид изложеното съдът заключава, че е бил постановен законосъобразен административен акт, който не подлежи на отмяна, а подадената срещу него жалба следва да бъде отхвърлена, като неоснователна.

При този изход на спора, на основание чл.143, ал.3 от АПК и чл.37, ал.1 от Закона за правна помощ и чл. 24 от Наредба за заплащането на

правната помощ, Агенция по заетостта следва да заплати на Комисията за защитна на личните данни сумата в размер на 100,00 (сто) лева, представляваща юрисконсултско възнаграждение за осъществено процесуално представителство.

Мотивиран от горното и на основание чл. 172, ал. 2 от АПК, ***Административен съд София-град***, II-ро отделение, 22-и състав,

Р Е Ш И :

ОТХВЪРЛЯ жалбата на Агенция по заетостта, представлявана от изпълнителния директор С. В., срещу ***решение № ПАИКД-13-2/2024 г. от 24.07.2024 г.*** на Комисията за защита на личните данни.

ОСЪЖДА Агенция по заетостта, представлявана от изпълнителния директор С. В., със седалище и адрес: [населено място], [улица] да заплати на Комисия за защита на личните данни с адрес: [населено място], [улица] сумата от 100,00 /сто/ лева на основание чл.143, ал.3 АПК.

РЕШЕНИЕТО подлежи на обжалване с касационна жалба в 14-дневен срок от получаване на съобщенията до страните за неговото постановяване, пред Върховния административен съд на Република България.

ПРЕПИСИ от акта да се изпратят и връчат на страните.

Съдия: