Р Е Ш Е Н И Е
№ 1229

гр. София, 13.01.2025 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **второ отделение 27 състав,** в публично заседание на 29.10.2024 г. в следния състав:

СЪДИЯ: Димитър Петров

при участието на секретаря Цветанка Митакева, като разгледа дело номер **7456** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145 и сл. от АПК, вр. чл.84 от Закон за защита на личните данни (ЗЗЛД).

Образувано е по жалба на Народното събрание на Република България срещу Решение на Комисията за защита на личните данни рег.№ ПАИКД-13-70/2022г. от 04.07.2024г., с което на основание чл.58, пар.2, буква „б“ от Регламент /ЕС/ 2016/679, за нарушение на чл.5, пар.1, буква „е“, вр. чл.32, пар.1, буква „б“ и буква „г“, е наложена принудителна административна мярка – „официално предупреждение“ на Народното събрание, в качеството му на администратор на лични данни за допуснато нарушение на разпоредбите на Регламента по уведомление за нарушение на сигурността на данните с вх.№ ПАИКД-13-70/09.11.2022г.

Жалбоподателят поддържа, че решението на КЗЛД е необосновано и незаконосъобразно. Поддържа, че Комисията е постановила акта си без да изпълни служебното си правомощие да събере всички относими доказателства и установи релевантните за случая обстоятелства. Поддържа, че изложените от КЗЛД мотиви са противоречиви и от тях не става ясно да е допуснато нарушение на сигурността на личните данни съгласно Регламент /ЕС/ 2016/679. Оспорва наложената ПАМ като нецелесъобразна, тъй като не е от естество да предотврати настъпването на подобен тип нарушение, доколкото са изложени мотиви, че неправомерният достъп до лични данни не е осъществен, чрез копиране на файлове от системата на НС, както и, че за

изпълнение на дадените предписания е необходим голям финансов ресурс, който е несъразмерен на тежестта на нарушението. Прави искане оспореният акт да бъде отменен.
Ответната по жалбата страна – Комисия за защита на личните данни, чрез своя пълномощник оспорва жалбата.
Софийска градска прокуратура не взема становище.
Съдът като прецени поотделно и в съвкупност събраните по делото доказателства и взе предвид доводите на страните, приема следното:
Административното производство пред КЗЛД е образувано въз основа на уведомление за нарушение на сигурността на личните данни по чл.33 от Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД), с вх.№ ПАИКД-13-70/09.11.2022г. подадено от НС на Р. България. Уведомлението се отнася за нарушение установено от администрацията на НС на 07.11.2022г., което се състои в публикуване на дискусионната страница на Сдружение „БОЕЦ“ на 8 документа, съдържащи незаличени лични данни – три имена, длъжност и саморъчните подписи на авторите на документите и други служители от администрацията на НС. В резултат на извършеното нарушение са засегнати данни на 29 лица – служители на администрацията на НС, контрагенти и служители на контрагенти. Конкретно документите представляват цветни копия на одитни доклади, становища, докладни записки и др.
Пред КЗЛД е образувана преписка, като за изясняване на обстоятелствата около нарушението, с писмо изх.№ ПАИКД-13-70#1/16.11.2022г. е изискана информация и документи НС, които са постъпили с писма от 21.11.2022г. и 23.11.2022г. От тях се установява, че на основание чл.12, ал.1 от Вътрешните правила за действие при нарушение на сигурността на личните данни на НС, е свикана Комисия за действие при нарушаване на сигурността на личните данни, определена със Заповед № АД 950-05-121/05.06.2019г., изм. със Заповед № АД-050-05-156/31.07.2020г. на Председателя на НС, която да извърши вътрешна проверка по случая. Извършена е цялостна вътрешна проверка, проследено е движението на документите и извършените оторизации за достъп до документите чрез ИИС на НС, като проверката е приключила на 16.11.2022г., а резултатите от нея са обективирани в протоколи. Извършени са оценка на риска, съгласно Методика за оценка на риска на НС; оценка на потенциалните последици от нарушението на сигурността за засегнатите субекти на данни, като всички засегнати служители на НС са били уведомени.
Констатирано е, че не са постъпили жалби или сигнали срещу администратора на лични данни, във връзка с нарушението на сигурността.
Събраните по преписката документи са докладвани на заседание на КЗЛД проведено на 30.11.2022г. Взето е решение за проверка на място, разпоредена със Заповед № РД-15-36/02.02.2023г. на Председателя на КЗЛД.
Изискано и получено е писмено становище от Сдружение „БОЕЦ“.
До НС е изпратен Въпросник за проверка с писмо от 10.02.2023г., като в отговор са получени комплект документи на 22.02.2023г.
Извършена е проверката на място, открита на 04.05.2023г. в сградата на НС. При проверката са присъствали длъжностни лица от администрацията на НС, като е отразено, че те са осигурили възможност за достъп и събиране на доказателства от страна на проверяващия екип.
За документиране на резултатите от проверката е съставен Констативен протокол, а

всички събрани материали в хода на извършената проверка са приложени към Констативен акт с вх.№ ППН-02-284/08.05.2024г. – актът и документите са приложени към административната преписка и са приети като писмени доказателства по делото.
При безспорна фактическа обстановка, КЗЛД е постановила обжалваното в настоящото производство Решение рег.№ ПАИКД-13-70/2022г. от 04.07.2024г.
Въз основа на събраните доказателства, Комисията е приела за установено, че администраторът на лични данни (НС) е предприел технически и организационни мерки за защита на личните данни. По отношение мерките за физическа защита е установено, че в обектите, в които се обработват лични данни са дефинирани границите на физическата сигурност и местата, които съдържат средства за обработка на лични данни и информация. Параметрите на физическата сигурност на информационните системи са определени в съответствие с Наредба на МС за минималните изисквания за мрежова и информационна сигурност. Помещенията, в които се разполага техническото оборудване, разполагат с технически системи за защита, безопасност и охрана, а физическият достъп до тях се регистрира в съответствие с Вътрешните правила за пропускателния режим в сградите на НС. Обособени са зони с контролиран достъп, който се осъществява със система за контрол на достъпа, СОТ система, въведени регистри за вписване на външни посетители с придружител, използват се детектори за субстанции. Определени са екип и комисия за реагиране при нарушения на сигурността на личните данни. В решението не са отбелязани констатирани нарушения при осигуряване на мерки за физическа защита при обработка на личните данни. Не са посочени забележки при осигуряване на персонална и документална защита – осигуряват се регулярни обучения по защита на личните данни; осъществява се контрол на достъпа до регистрите с лични данни посредством оторизация; съществуват правила за размножаване и разпространение на документи, а документите по одитните ангажименти се обработват и съхраняват съгласно изискванията на Закона за вътрешния одит в публичния сектор (ЗВОПС) – резултатите от изпълнението на всеки одитен ангажимент за увереност и консултиране се документират, обсъждат и докладват на ръководителя на организацията и с ръководителите на структурите, чиято дейност е одитирана. Уредено е, достъпът до документи и информация по одитните ангажименти за външни за НС структури и лица, да се предоставя само след одобрение и разпореждане от Председателя на Народното събрание. Утвърдени са и правила за съхранение и унищожаване на лични данни, по отношение на които също не са констатирани нарушения.
По отношение защита на АИС/мрежа и криптографска защита, са направени констатации, че съгласно Политика за мрежова и информационна сигурност в информационните системи на НС, е заложен сигурен механизъм за контрол на достъпа, включващ еднозначна идентификация на потребителя, контрол на правомощията, регистриране на всички действия на потребителя. Достъпът до ИИС на НС се осъществява чрез уникално потребителско име и парола като се създават акаунти за достъп на конкретния служител. Отдаленият достъп до системните ресурси на НС се осъществява чрез криптиран канал – Virtual Private Network (VPN), като се използва защита чрез лицензиран антивирусен софтуер, управляван централизирано, който е инсталиран на всички работни локални станции и преносими компютърни системи. Системата се управлява само от администраторите на системата. Въведени са специални правила при работа с електронна поща. Извършена

е проверка от министерство на електронното управление във връзка с управление на мрежовата и информационна сигурност, като не са издадени препоръки.
Проверяващите са констатирали и, че в съответствие с изискванията на чл.24, пар. 2 от Регламента, администраторът е утвърдил необходимите вътрешни документи, в които са определени основните принципи и цели при обработване на личните данни.
Въз основа на тези констатации от извършената проверка административният орган е обективирал извод, че е налице нарушение на поверителността на личните данни, изразяващо се в тяхното разкриване пред получатели (неограничен кръг лица), които не са оправомощени да ги получат и/или да имат достъп до същите. Към момента на проверката е констатирано, че оригиналите на документите, предмет на нарушението на сигурността, се намират на хартиен носител в архива на НС, в изолирано помещение с контролиран достъп. Същите документи се намират в електронен вид, във файлов формат pdf, в ИИС на НС, като са сканирани в системата черно-бяло. В тази връзка е направен извод, че след като документите качени на уебсайта на Сдружение „БОЕЦ“, са цветни, следва че те представляват цветни копия на оригиналите на документите, а не копие на документите, съхранявани в електронен вид в ИИС на НС. Въпреки този извод, административният орган приема, че липсва механизъм за установяване на конкретното лице, което е достъпвало, „разпечатило“ и предало документите за публикуването им на уебсайта, тъй като не е наличен конфигуриран PaperCut сървър или друго софтуерно решение, което да служи за сигурност, контрол и управление на печатната среда. Не са налични регистрационни файлове (Log files) от работните станции и периферните устройства в помещенията, в които са се съхранявали въпросните документи, предмет на нарушението, а ИИС на НС не е конфигурирана да идентифицира конкретен файл, на кой компютър (работна станция) е отворен, дали същият е принтиран и/или качен на преносим носител. Посочено е и, че администраторът извършва оценка на риска веднъж годишно, съгласно утвърдена Методика. Констатирано е, че е извършван одит на информационните системи преди осъществения нерегламентиран достъп, като са изготвени одитен доклад и оценка на риска на дейностите по обработка на личните данни, които документи са предоставени на КЗЛД, във връзка с подадено предходно уведомление по Регламента от 05.08.2020г. и следва изводът, че в „оценките, изводите и препоръките, в резултат на извършените одити, не са отразени факти и обстоятелства по отношение на възникналото събитие, предмет на настоящата проверка от страна на КЗЛД“.
В частта от акта, съдържащ правните изводи, административният орган е приел, че са нарушени разпоредбите на чл.5, пар.1, буква „е“ и чл.32, пар.1, буква „б“ и пар.2 от Регламент (ЕС) 2016/679 – че данните са обработени от администратора по начин, който не генерира в достатъчна степен подходящо ниво на сигурност на обработването, което да осигури постоянна поверителност на личните данни. Добавено е, че независимо от констатациите при осъществените проверки (предприетите своевременно от администратора мерки за предотвратяване на достъпа до данните, намаляване на рисковете, преодоляване на последствията от нарушението и недопускане на ново такова, както и, че не са установени други случаи на нарушения), предвид установяването на посоченото нарушение и пробива в сигурността на изнесените данни, е необходимо да бъдат своевременно предприети такива технически и организационни мерки за спазване на правилата на Регламента, които да бъдат съответни на констатираните рискове и заплахи от нерегламентирано

разпространение на лични данни. Направен е извод, че тези пропуски могат да бъдат преодолени с въвеждане на електронно деловодство при ограничаване на отпечатването на документи и тяхното резолиране на единен вход/изход на документооборота. С тези мотиви е формулирана диспозитивната част на акта, с която на основание чл.58, пар.2, буква „б“ от Регламент /ЕС/ 2016/679, за нарушение на чл.5, пар.1, буква „е“, вр. чл.32, пар.1, буква „б“ и буква „г“, е наложена принудителна административна мярка – „официално предупреждение“ на Народното събрание, в качеството му на администратор на лични данни за допуснато нарушение на разпоредбите на Регламента по уведомление за нарушение на сигурността на данните с вх.№ ПАИКД-13-70/09.11.2022г.

В съдебното производство не са ангажирани нови доказателства.

При така установената фактическа обстановка, съдът намира от правна страна следното:

Обжалва се решение на КЗЛД, с което е приложена мярка по чл. 58, параграф 2, буква „б“, от Регламент (ЕС) 2016/679. Решението на Комисията, на основание чл.38, ал.8 от ЗЗЛД подлежи на обжалване по реда на АПК.

Съгласно правомощията си по чл.146 АПК съдът при преценка законосъобразността на административния акт проверява дали е издаден от компетентен орган (т.1), в съответната форма (т.2), допуснато ли е съществено нарушение на административно-производствени правила при издаването му (т.3), налице ли е противоречие на административния акт с материалноправни разпоредби (т.4) и несъответствие с целта на закона (т.5), като съдът не е ограничен от посочените от оспорващия основания, а проверява всички основания по чл.146 АПК.

Съответствието на оспорения акт с материалния закон се преценява към момента на издаването на административния акт (чл.142, ал.1 АПК).

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. Съгласно чл. 7, ал. 1 от ЗЗЛД комисията е колегиален орган и се състои от председател и 4 членове, а решенията се вземат с мнозинство от общия брой на членовете - чл. 9, ал.3. В случая оспореното решение е взето с необходимото мнозинство – председател и трима членове, с оглед на което същото е валидно.

Оспореният акт обаче е необоснован, не отговаря на законоустановените изисквания за форма и мотивираност, както и при издаването му са нарушени процесуалните правила.

Административният акт задължително съдържа фактически и правни основания за издаване на акта, както и ясна разпоредителна част, която съответства на установените от органа обстоятелства и посоченото от него правно основание за издаване на акта – чл.59, ал.2, т.4 и 5 от АПК.

В конкретния случай, в обжалваното Решение на КЗЛД рег.№ ПАИКД-13-70/2022г. от 04.07.2024г. е налице явно противоречие в мотивите на административния орган – противоречие между приетите за установени обстоятелства и наложената ПАМ – необходимостта от предприемане на конкретни действия с цел предотвратяване и преустановяване на нарушението при обработване на лични данни, както и за предотвратяване и отстраняване на вредните последици от него. В решението, административният орган е достигнал до категоричния извод, че разпространените в интернет пространството документи съдържащи лични данни, представляват цветни копия на оригиналите на документите, които оригинали се намират на хартиен

носител в архива на НС, в изолирано помещение с контролиран достъп. Въпреки тези обстоятелства - че е приел, че се касае за цветно копие на оригиналните документи, органът с обжалвания акт е мотивирал решението си за налагане на ПАМ с извода, че липсва механизъм за установяване на конкретното лице, което е достъпвало, „разпечатило“ и предало документите за публикуването им на уебсайта. Никъде обаче, не се твърди документите да са разпечатвани от електронната система на администратора. Напротив, в решението е посочено, че тези документи действително се намират в електронен вид, във файлов формат pdf, в ИИС на НС, но тъй като в електронен вид те са сканирани в системата черно-бяло, няма как качените на уебсайта документи – цветни, да са били разпечатани от ИИС на НС. Въпреки това, в противоречие с тези изводи за установените обстоятелства с обжалваното решение като основание за налагане на ПАМ, органът е приел, че липсва механизъм за установяване на конкретното лице, което е достъпвало, „разпечатило“ и предало документите за публикуването им на уебсайта, както и, че този пропуск може да се преодолее при наличието на конфигуриран PaperCut сървър или друго софтуерно решение, което да служи за сигурност, контрол и управление на печатната среда, както и ИИС на НС да е конфигурирана да идентифицира конкретен файл, на кой компютър (работна станция) е отворен, дали същият е принтиран и/или качен на преносим носител. Противоречието между приетите за установени фактически обстоятелства (че нерегламентираният достъп до лични данни е осъществен, чрез копия на оригиналите на документите) и посочените подходящи мерки за предотвратяването им – чрез конфигуриране на сървър и ИИС на НС, при посочен извод, че няма нерегламентиран достъп до сървъра и ИИС, водят до съществен порок във формата на административния акт, обуславящ извод за неговата незаконосъобразност.

Отделно от това, административният орган е изложил констатация, че „оценките, изводите и препоръките, в резултат на извършените одити, не са отразени факти и обстоятелства по отношение на възникналото събитие, предмет на настоящата проверка от страна на КЗЛД“, но тази констатация се сочи, че е на база одитен доклад и оценка на риска на дейностите по обработка на личните данни, които документи са предоставени на КЗЛД, във връзка с подадено предходно уведомление по Регламента от 05.08.2020г., а процесното е от 09.11.2022г. В тази връзка необоснован се явява изводът на КЗЛД, че в годишните одитен доклад и оценка на риска изготвяни от администратора, не са отразени факти и обстоятелства по отношение на възникналото събитие, тъй като в нарушение на процесуалните правила, не са изискани релевантните за периода одитен доклад и оценка на риска, за които в жалбата пред съда се твърди, че са взети предвид обстоятелствата свързани с процесното събитие.

В обжалвания акт липсват конкретни мотиви, с оглед установените обстоятелства необходимо ли е да се прилага мярка по чл.58, пар.2, от Регламент /ЕС/ 2016/679, които мерки съгласно чл.84, ал.1 ЗЗЛД са ПАМ по ЗАНН, и каква конкретна мярка ще изпълни изискванията на чл.22 ЗАНН – да послужи предотвратяване и преустановяване на конкретно нарушение, както и за предотвратяване и отстраняване на вредните последици от него.

Последователно се застъпва е практиката на Съда на ЕС, в това число и в Решение на Съда (първи състав) от 26 септември 2024 година по дело C-768/21, че не може да се изключи, че по изключение и предвид особените обстоятелства на конкретния случай надзорният орган може да се въздържи от приемането на корективна мярка, въпреки че е установено нарушение на сигурността на личните данни. Такъв би могъл да бъде по-специално случаят, когато установеното нарушение не е продължило, например когато администраторът, който по принцип е приложил

подходящи технически и организационни мерки по смисъла на член 24 от ОРЗД, веднага след като е узнал за това нарушение, е предприел подходящи и необходими мерки, за да се преустанови посоченото нарушение и за да не бъде отново извършено, като се имат предвид задълженията му, произтичащи по-специално от член 5, параграф 2 и член 24 от този регламент.
В тази връзка в обжалваното решение органът не е изложил никакви мотиви, дали с оглед установените обстоятелства изобщо следва да се налага корективна мярка по чл.58 от Регламента, предвид изричните възражения на администратора основаващи се на установените обстоятелства за предприети действия за осигуряване на спазване изискванията на регламента и своевременно докладване на случая (критериите в цитираното по-горе решение по дело C-768/21) и липса на други нарушения, в това число и жалби на засегнати лица. По тези възражения, органът дължи конкретни мотиви. Ако приеме, че следва да се наложи корективна мярка, органът следва да се мотивира като изложи отново конкретни съображения, че избраната мярка е за постигане целта, преследвана с член 58, параграф 2 от ОРЗД - чрез намесата на националните надзорни органи с прилагане на конкретна мярка ще се гарантира съответствието на обработването на лични данни с регламента и отстраняването на нарушения на последния, за да се постигне съответствие с правото на Съюза (решение от 14 март 2024 г., Ъjpesti Polgбrmesteri Hivatal, C-46/23, EU:C:2024:239, т. 40).
Противоречията в мотивите на обжалвания акт, нарушението на процесуалните правила довело до неизясняване на всички относими обстоятелства, липсата на ясни и категорични мотиви по отношение конкретните възражения на администратора, че с оглед конкретните обстоятелства, не следва изобщо да се налага мярка по чл.58, пар.2 от Регламента, както и ако органът приема, че мярка следва да се наложи – липсата на ясни мотиви каква конкретно мярка е необходима за да се преустанови конкретното нарушение и предотврати възможността за извършване в бъдеще на същото такова, водят до извод за незаконосъобразност на административния акт. Жалбата срещу него е основателна и следва да бъде уважена.
Решение на КЗЛД рег.№ ПАИКД-13-70/2022г. от 04.07.2024г., следва да бъде отменено, а преписката изпратена на административния орган за ново разглеждане и произнасяне при спазване на дадени по-горе указания – за изясняване на всички относими обстоятелства в това число дали в изготвените от администратора одитен доклад и оценка на риска, за относимия период, са отразени факти и обстоятелства по отношение на възникналото събитие, предмет на настоящата проверка от страна на КЗЛД, както и след изясняване на всички обстоятелства да се произнесе с акт по чл.84 ЗЗЛД, който съдържа фактически и правни основания за издаване на акта, както и ясна разпоредителна част, която съответства на установените от органа обстоятелства и посоченото от него правно основание за издаване на акта. В частност, да посочи конкретни съображения във връзка с възраженията на администратора дали с оглед всички обстоятелства свързани с нарушението следва да се налага мярка по чл.58, пар. 2 от Регламента, като съобрази предприетите действия за осигуряване на спазване изискванията на регламента и своевременното докладване на случая (критериите в цитираното по-горе решение по дело C-768/21) и липса на други нарушения, в това число и жалби на засегнати лица. Ако органът приеме, че са налице основания за прилагане на мярка, следва да изложи мотиви и какви конкретно действия следва да предприеме администратора за да осигури спазването изискванията на регламента, с оглед конкретното нарушение – нерегламентиран достъп до цветни копия на оригиналите на документи, съхранявани в архива на НС.
На основание чл.174 АПК, следва да се определи срок от един месец за издаване на

акта по чл.84 ЗЗЛД.
По отговорността на страните за разноски:
При този изход на делото право на разноски на основание чл.143, ал.1 АПК има жалбоподателят, като в негова полза следва да се присъдят сторените разноски от 50 лв. – платена държавна такса и 100 лв. – юрисконсултско възнаграждение, определено на основание чл.37 от ЗПрП.
Воден от горното, Административен съд София град, 27 състав

Р Е Ш И:

ОТМЕНЯ по жалба на Народното събрание на Република България, Решение на Комисията за защита на личните данни рег.№ ПАИКД-13-70/2022г. от 04.07.2024г.
ИЗПРАЩА преписката на Комисията за защита на личните данни за ново разглеждане и произнасяне с акт по чл.84 ЗЗЛД, в едномесечен срок от влизане в сила на настоящото решение, при спазване на дадените указания.
ОСЪЖДА Комисията за защита личните данни, **да заплати** на Народното събрание на Република България, на основание чл.143, ал.1 АПК, сумата 50 лева – съдебни разноски, както и сумата от 100 лева – юрисконсултско възнаграждение.
Решението подлежи на обжалване с касационна жалба пред Върховния административен съд, в 14-дневен срок от съобщаването му на страните.

СЪДИЯ: