Р Е Ш Е Н И Е
№ 2762

гр. София, 25.04.2024 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 59 състав,** в публично заседание на 11.04.2024 г. в следния състав:

СЪДИЯ: Зорница Дойчинова

при участието на секретаря Светла Гечева, като разгледа дело номер **1633** 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/, във вр. с чл. 38, ал. 7 от Закона за защита на личните данни /ЗЗЛД/.

Образувано е по подадена жалба от „Сибериан Уолф“ ООД, чрез адв. М., срещу решение № ПАИКД-13-40/2022 от 08.01.2024 г. на Комисията за защита на личните данни /КЗЛД/, с което на „Сибериан Уолф“ ЕООД, в качеството му на администратор на лични данни, на основание чл. 58, § 2, б. „г“ от Регламент (ЕС) 2016/679, за нарушение на чл. 5, § 1, б. „е“, вр. чл. 32, § 1, б. „б“ и б. „г“ и чл. 5, § 2 от Регламент (ЕС) 2016/679, е разпоредено да предвиди в своите вътрешни документи извършване на периодичен анализ за риска (като се определи конкретен повод, през който същият да бъде извършван), а в случай на въвеждане на нови технологии да бъде задължителен; да предвиди в своите вътрешни документи спазване на принципите на отчетност, което разпореждане да бъде изпълнено в рамките на три месеца от влизане в сила на решението, както и на основание чл. 58, § 2, б. „и“ от Регламент (ЕС) 2016/679 му е наложено административно наказание „имуществена санкция“ в размер на 10 000 (десет хиляди) лева съгласно чл. 83, § 4, б. „а“ за нарушение на чл. 25, чл. 28, чл. 32, § 1, б. „б“ и б. „г“ от Регламент (ЕС) 2016/679 и чл. 83, § 5, б. „а“ за нарушение на чл. 5, § 2 от Регламент (ЕС) 2016/679.

В жалбата са изложени съображения за нищожност на оспореното решение, представляващо, според жалбоподателя, общ административен акт. Посочва, че решението е постановено при липса на компетентност и при неосигуряване на

законовопредвидения кворум. Твърди липса на мотиви, обосноваващи избора на наложените от КЗЛД мерки и санкции. Аргументира съществено нарушение на административнопроизводствените правила, изразяващо се в неуведомяването от страна на КЗЛД на дружеството или негов представител за датата на заседанието, на което е взето процесното решение. Така администраторът на лични данни е лишен от възможността да изрази позицията си във връзка с определяне размера на административното наказание, наличието на смекчаващи отговорността обстоятелства и други релевантни факти, имащи значение за индивидуализацията на наказанието. Отделно от това, при постановяване на процесното решение, надзорният орган не е съобразил в цялост приложените по административната преписка документи, доказателства, отговори и становища от страна на дружеството, по-конкретно отговор от 31.03.2023 г., видно от който физическите лица, изработили информационната система (уебсайта) – www.wolfintech.com, са имали достъп единствено до информацията, която се е съхранявала в уебсайта, а именно име и адрес за електронна кореспонденция (e-mail) на съответния субект – клиент на дружеството. Всички останали данни, упоменати в уведомлението за нарушение, като паспортни данни, ЕГН, адрес, месторождение, телефонен номер, са съхранявани в специализирана платформа за обработване и съхранение на данни, до която достъп е имал единствено управителят на дружеството. Твърди също, че към момента на инцидента дружеството е разполагало с разписани вътрешни правила за обработване на личните данни, приети на 01.03.2022 г. и приложени по административната преписка с отговор от дружеството от 18.12.2022 г. Излага доводи за противоречие на решението с материалния закон и с целта на закона. Моли за прогласяване на нищожността на оспореното решение. Алтернативно, моли за отмяната му. Претендира разноски.

В съдебно заседание, жалбоподателят се представлява от адв. М., който моли за уважаване на жалбата по съображенията, изложени в нея. Моли съдът да обяви за нищожно процесното решение на КЗЛД, поради липса на компетентност и съществено нарушение на административнопроизводствените правила, или алтернативно да се отмени решението като незаконосъобразно. Алтернативно моли да се намали санкцията. Заявява, че не претендира разноски.

Ответникът – Комисия за защита на личните данни, чрез процесуалния представител К., в представено писмено становище излага подробни съображения за неоснователността на жалбата. Излага доводи за липса на процесуални нарушения и съответствие на оспорения административен акт с материалния закон, както и съответствие с целта на закона. Оспорва жалбата и моли за нейното отхвърляне. Моли за присъждане на юрисконсултско възнаграждение. Прави възражение за прекомерност на адвокатското възнаграждение.

В съдебно заседание не се представлява.

СГП не изпраща представител и не взима становище по жалбата.

Административен съд София-град, в настоящия съдебен състав, след като обсъди доводите на страните и прецени по реда на чл. 235, ал. 2 от ГПК, във вр. с чл. 144 от АПК приетите по делото писмени доказателства, приема за установено от фактическа страна следното:

С уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент (ЕС) 2016/679, с вх. № ПАИКД- 13-40/14.07.2022 г., „Сибериан Уолф“ ООД е сезирало КЗЛД. В уведомлението е изложено, че във връзка с изпълнение на търговската си

дейност, свързана с виртуални валути, дружеството възлага на трети лица да изработят уебсайт: www.wolfintech.com, чрез който клиентите на дружеството да използват услугите, които то предлага, във връзка с виртуални валути и поверяване на криптовалута, като работата е била възложена на основание устни договорки между страните, при условията на добросъвестно сътрудничество и колегиалност във взаимоотношенията, без да е сключен договор в писмена форма. След изработването и въвеждането в експлоатация на информационната система и осигуряването на достъп на клиенти на дружеството да създават регистрационни акаунти за ползване на услугите на дружеството, дружеството е изискало от лицата, изработили сайта, да предоставят всички пароли, кодове, ключове за достъп и администриране на сайта (www.wolfintech.com) и бек-енд компонентите. След като не е получен доброволно и незабавно достъпа и контрола върху сайта, поради несъгласие на лицата, изработили сайта да ги предоставят, дружеството счело, че е налице нерегламентиран достъп от страна на същите до всички данни на субектите — клиенти на администратора.

Посочено е, че от създаването през месец март 2022 г. на сайта, до 27.06.2022 г., „Сибериан Уолф“ ООД, в качеството му на възложител за изработване на уебсайта, не е разполагало с никакъв достъп до данни за администриране на сайта, пароли, кодове, ключове за достъп и не е било в състояние да използва и да управлява информационната си система, не е имало достъп за администриране, обработване и съхранение на информационните данни в сайта, в това число договорна информация и лични данни на контрагенти „Сибериан Уолф“ ООД, която се съдържа в информационната система www.wolfmtech.com.

На 27.06.2022 г., след многократни молби и усилия от страна на дружеството и след официално писмено уведомление и покана, един от разработчиците е предоставил списък с данни и пароли за достъп до информационната система, който не е бил изчерпателен, като за пълен достъп до ресурсите на сървъра, където е инсталирана информационната система, се изисквало допълнителен код за верификация (проверка) на достъпа, който код се изпраща до чужд за администратора телефонен номер при всеки опит за достъп до сайта. Поради тази причина е било невъзможно използването и администрирането на информационната система в пълен обем, тъй като са били поставени в техническа невъзможност за това. На 04.07.2022 г. дружеството установило, че кодът за достъп до системата за управление на съдържанието на сайта (WordPress.com) е променен от трето лице без тяхно съгласие. Това потвърждавало факта, че е налице нерегламентиран достъп от страна на трето лице до информационна система (уебсайт) и администраторът все още не е имал пълен достъп и контрол над системата и всички данни, които се съдържат в нея.

Посочено е, че е извършена вътрешна проверка във връзка с възникналия инцидент, като не са установили неправомерно придобиване, съхранение или разпространение на лични данни на клиентите. Предвид обстоятелството обаче, че лицата, които са изработили и администрирали сайта, са имали достъп до цялата информация и данни, които се съдържат и съхраняват в сайта и предвид факта, че тези лица не са предоставили доброволно в определения за това срок всички пароли и ключове за достъп, можело да се заключи, че е налице риск от евентуално недобросъвестно използване на голям обем лични данни. В тази връзка, след неколкократни покани към лицата, изработили сайта, да предадат на дружеството всички пароли и ключове за достъп и администриране на сайта и след провеждани преговори с тях, както и с помощта на експертен технически (IT) екип, дружеството е успяло да се снабди с

пълен достъп до информационната система и до всички съхранявани данни за клиенти на дружеството, както и да преустанови всякакви възможности за неправомерна намеса и достъп от трети лица. Данните се съхраняват на защитен носител (в защитено облачно пространство), като преноса на данните е осъществен с помощта на експертен технически (IT) екип.
Засегнати от нарушението субекти на данни са общо 129 физически лица, от които 126 физически лица - граждани на Италия; 1 физическо лице - гражданин на Румъния; 1 физическо лице - гражданин на М.; 1 физическо лице - гражданин на България. А категориите лични данни, засегнати от нарушението са били: имена, ЕГН, копие на лична карта, месторождение, телефон, е-мейл, произход (расов, етнически), имотно състояние, финансово състояние, произход на активи, собственоръчно направена от субекта снимка на лице, с цел идентифициране и доказване на идентичност на субекта с лицето, чиито паспортни данни са предоставени.
За изясняване на фактите от значение за случая, с писмо на КЗЛД, изх. № ПАИКД-13-40#1/29.07.2022 г., от „Сибериан Уолф“ ООД е изискана информация и относими документи.
С писмо вх. № ПАИКД-13-40#3/Ю.08.2022 г., в КЗЛД са постъпили от дружеството допълнителни документи и информация.
С Докладна записка, рег. № ПАИКД-13-40#4/02.09.2022 г., постъпилото уведомление е докладвано на заседание на КЗЛД, проведено на 07.09.2022 г. и е прието Решение за извършване на проверка на място, поради наличие на „високо ниво на риск“ за правата и свободите на физическите лица.
Със заповед № РД- 15-73/03.03.2023 г. на председателя на КЗЛД е разпоредено извършване на проверка на място на администратора на лични данни „Сибериан Уолф“ ООД. Със същата заповед е определен екип, който да извърши проверката, както и основната задача - установяване на факти и обстоятелства, във връзка с получено уведомление за нарушение на сигурността на личните данни по чл. 33 от Регламент ЕС 2016/679.
С писмо, изх. № ПАИКД-13-40#15/17.02.2023 г., е изпратено уведомление до дружеството относно предстоящото извършване на проверка на 07.03.2023 г.
Въз основа на извършената проверка, от проверяващия екип е съставен Констативен акт /КА/ с рег. № ППН-02-439/06.07.2023 г., в който е отразено, че „Сибериан Уолф“ ООД, в качеството на „администратор на лични данни“ по смисъла на чл. 4, т. 7 от Регламент (ЕС) 2016/679, е допуснал нарушаване на сигурността при осъществяване на дейността си, а именно: загубил е контрол над личните данни, които са събирани и обработвани от негово име - лицата разработили интернет страницата - www.wolfmtech.com са имали пълен контрол над нея, в това число на съдържащите се там лични данни, без съгласието на администратора. Описаното нарушение на сигурността в Уведомление за нарушение на сигурността № ПАИКД-13-40/14.07.2022 г. говори, че „Сибериан Уолф“ ООД не е предприело 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 определял кои мерки са подходящи, администраторът следвало 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, „Сибериан Уолф“ ООД е следвало да приложи подходящи технически и организационни мерки за осигуряване на съобразено с конкретните рискове ниво на сигурност. Това е залегнало и в задължението, визирано в нормата на чл. 25 от Регламент (ЕС) 2016/679, която се отнася до защитата на личните данни на етапа на проектиране и по подразбиране. Изпълнението на това задължение, както и задължението за въвеждането на подходящи технически и организационни мерки, съгласно чл. 32, параграф 1 от Регламент (ЕС) 2016/679 са условия, които гарантират съответствие с принципа за цялостност и поверителност (чл. 5 параграф 1, буква „е“ от регламента).

В КА е посочено още, че отговорност на „Сибериан Уолф“ ООД, съгласно чл. 5, § 2 от регламента (принцип за отчетност), е да докаже спазването на принципите за обработване на данни, дефинирани в § 1 на същия член. Във връзка с това, администраторът следвало надлежно да документира всички процеси по обработване на личните данни. Необходимо е било да се създава документална среда относно обработването на личните данни - да разполага с писмени документи, които да позволяват проследимост на процесите по обработване на данните.

Отразено е също, че когато за обработването на лични данни администратор ползва услугите на обработващ личните данни, следва да се спазват нормите на чл. 28 от регламента, като използва обработващ, който предоставя достатъчни гаранции за прилагането на подходящи технически и организационни мерки. Отношенията с обработващият следвало да са уредени с договор или друг правен акт, който има задължителен характер и регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на обработващия и на администратора. А в случая, от дружеството не са предприети не действия с цел обработването да протича в съответствие с изискванията на регламента и не било в състояние да докаже спазване изискванията на чл. 28 от Регламент (ЕС) 2016/679.

В заключение е посочено, че администраторът е допуснал разработването и предприемането на технически мерки за сигурност от лица, с които не е имал сключен договор, в който да бъдат указани какви техническите и организационни мерки следва да се предприемат при разработване и внедряване на интернет страницата - www.wolfintech.com. Във връзка с дейността си администраторът е следвало да събира и обработва голям обем от лични данни на своите клиенти, включително такива, с достъпването на които за лицата могат да настъпят сериозни финансови загуби. Прието е, че дружеството не е оценило рисковете с различна вероятност и тежест за правата и свободите на физическите лица. Предвид факта, че не е имало ясни правила и критерии по отношение на техническите и организационни мерки при изработване на интернет страницата, администраторът е допуснал, лицата разработили същата, да имат безконтролен достъп до предоставените данни, като за този период не е могъл да осигури и съответната сигурност и гаранции за законосъобразното обработване на предоставените от клиентите данни. Това е потвърдено и от Dracteam Technology LLC, които са извършили проверка и оценка на състоянието на активите на www.wolfmtech.com. След настъпване на инцидента е преустановено предоставянето на услуги чрез сайта www.wolfintech.com, като дружеството е предприело действия по изработване на изцяло нова информационна платформа, за да продължи да предоставя своите услуги на клиенти.

На закрито заседание, проведено на 13.09.2023 г. на КЗЛД, отразено в Протокол № 30/13.09.2023 г., е разгледана и обсъдена преписка с рег. № ПАИКД-13-40/14.07.2022 г. На това заседание е взето единодушно решение, като преписката е приключила с постановяване на Решение рег. № ПАИКД-13-40/2022 г. на КЗЛД, с което: т. 1. на основание чл. 58, § 2, буква „г" от Регламент (ЕС) 2016/679 за нарушение на чл. 5, § 1, буква „е“ във връзка с чл. 32, § I, буква „б“ и буква „Г“ и чл. 5 § 2 от Регламент (ЕС) 2016/679 е разпоредено на администратора лични данни „Сибериан Уолф“ ООД: Да предвиди в своите вътрешни документи извършване на периодичен анализ на риска (като се определи конкретен период, през който същият да бъде извършван), а в случай на въвеждане на нови технологии да бъде задължителен; Да предвиди в своите вътрешни документи спазване на принципите на отчетност; като е даден срок разпореждането да бъде изпълнено в рамките на 3 (три) месеца от влизане в сила на решението, след което в 14 (четиринадесет) дневен срок, администраторът да уведоми Комисията за защита на личните данни за неговото изпълнение, като представи съответните доказателства; по т. 2. На основание чл. 58, § 2, буква „и“ от Регламент (ЕС) 2016/679, е наложено на администратора „Сибериан Уолф“ ООД административно наказание имуществена санкция в размер на 10 000 (десет хиляди) лева, съгласно чл. 83, §, 4 буква „а“, за нарушение на чл. 25, чл. 28, чл. 32, § 1, буква „б“ и буква „г“ от Регламент (БС) 2016/679 и чл. 83, § 5, буква „а“ за нарушение на чл. 5, § 2 от Регламент (ЕС) 2016/679.

В мотивите на решението е прието, че в конкретния случай трети лица са имали достъп до масивите с лични данни на администратора, както и възможност безпрепятствено да ги придобият. Поради факта, че администраторът не е предприел необходимите технически и организационни мерки, третите лица са имали достъп до данни за 129 физически лица субекти на лични данни. Комбинацията от лични данни, до които третите лица са имали достъп, позволява засегнатите субекти на данни да бъдат идентифицирани лесно, без да са необходими допълнителни усилия: Основни данни - имена; ЕГН, копие на лична карта, месторождение, телефон, е-мейл, снимка на лицето с цел идентифициране и доказване на идентичност със субекта, чиито паспортни данни са предоставени; чувствителни данни - расов, етнически произход; финансови данни - имотно състояние, финансово състояние, произход на активи. Посочено е, че администраторът на лични данни „Сибериан Уолф“ ООД не е извършил анализ на риска преди нарушението на сигурността на личните данни, в следствие на което администраторът не се е съобразил с принципите за защита на данните на етапа на проектирането и защита на данните по подразбиране, съобразно разпоредбите на чл. 25 от Регламент (ЕС) 2016/679, съответно не е предприел подходящи технически и организационни мерки, което е довело до възникване на разглеждания инцидент. По този начин администраторът е нарушил чл. 5, § 1, буква „е“ във връзка с чл. 32, параграф 1, буква “г“ от Регламент (ЕС) 2016/679, като не е извършил анализ и оценка на ефективността на техническите и организационни мерки, за да гарантира сигурност на обработването. Посочено е също така, че към момента на възникване на инцидента, администраторът не е разполагал с разписани вътрешни правила за обработване на личните данни, свързани със специфичния предмет на дейност на „Сибериан Уолф“ ООД. Във връзка с горепосоченото администраторът не доказва спазването на чл. 5, § 1 от Регламент (ЕС) 2016/679, като по този начин е реализирано нарушение на „принципа за отчетност“ по чл. 5, § 2 от регламента. Прието е, че „Сибериан Уолф“ ООД не е спазил разпоредбите на чл. 28,

като е възложил чрез устна договорка и при липсата на ясни критерии за избор на изпълнител, който да изработи сайта на дружеството www.wolfintech.com. Не е сключен писмен договор, който ясно н подробно да регулира отношенията между дружеството и изпълнителите, които са разработили сайта www.woIftntech.coni, както и да регулира как и на какъв етан дружеството ще има пълен достъп до своя уебсайт. Не са договорени също и отговорността и санкциите спрямо разработчиците на сайта www.wolfintech.com в случай на неизпълнение, включително и по отношение законосъобразността на действията, свързани с обработваните лични данни.
Прието е още в мотивите на решението, че посредством засегнатите данни, лицата може недвусмислено да бъдат идентифицирани, съответно потенциалното въздействие върху субектите на данни може да доведе до загуба на контрол над личните им данни, също и загуба на поверителност на личните данни на засегнатите субекти. Нарушението е извършено умишлено, както и че от страна на администратора не са били предприети достатъчно подходящи технически и организационни мерки за запазване поверителността на личните данни е допринесло в голяма степен за реализиране на нарушението. В конкретния случай, администраторът на лични данни в пълна степен, носи отговорност за настъпването на нарушението на сигурността на личните данни, тъй като не е предприел подходящи технически и организационни мерки за защита поверителността на личните данни още на етапа на проектирането.
При определяне съответния размер на имуществената санкция, КЗЛД е взела предвид, че към датата на заседанието на комисията - 13.09.2023 г., на което е взето решението, годишният финансов отчет на „Сибериан Уолф“ ООД за финансовата 2022 г. все още не е бил обявен в търговския регистър, което задължение следва да бъде изпълнено до 30.09.2023 г. Поради това, КЗЛД е определила размер на санкцията, който клони към минимален размер - 10 000 (десет хиляди) лева, равняваща се приблизително на 5 000 (пет хиляди) EUR.
Решението е съобщено на представител на жалбоподателя на 29.01.2024 г.
Жалбата е подадена на 09.02.2024 г.

При така установените факти, настоящия съдебен състав на АССГ, като извърши цялостна проверка за законосъобразността на оспорения индивидуален административен акт на всички основания по чл. 146 от АПК, по реда на чл. 168, ал. 1 от АПК, достигна до следните правни изводи:
Предмет на оспорване е решение № ПАИКД-13-40/2022 от 08.01.2024 г. на КЗЛД.
Жалбата е подадена от лице, имащо правен интерес от оспорване на акта, тъй като жалбоподателя е адресат на процесното решение, поради което с акта са засегнати негови права и законни интереси. Жалбата е в срока за обжалване на индивидуалните административни актове, за което са представени надлежни доказателства. Жалбата е насочена срещу годен за оспорване административен акт, поради което следва да бъде разгледана по същество.
Съгласно изискванията на чл. 168, ал. 1 от АПК, при служебния и цялостен съдебен контрол за законосъобразност, съдът извършва пълна проверка на обжалвания административен акт относно валидността му, спазването на процесуалноправните и материалноправните разпоредби по издаването му и съобразен ли е с целта, която преследва законът, т. е. на всички основания, визирани в чл. 146 от АПК. При преценката си, съдът изхожда от правните и фактическите основания, посочени в

оспорвания индивидуален административен акт, представената административна преписка и събраните по делото доказателства. При проверката на административния акт, съдът не е обвързан от основанията, въведени от оспорващия, нито от неговото искане. Съдът следва да отмени или обяви за нищожен акта и ако констатира порок, който оспорващият не е посочил.

Разгледана по същество е неоснователна.

По съответствие на заповедта с процесуалните правила:

Съгласно чл. 6, ал. 1 от ЗЗЛД, 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.

Оспореният акт е издаден от компетентен орган, в кръга на неговите правомощия, съгласно чл. 10 от ЗЗЛД. Съгласно цитираната разпоредба, 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 на административния съд. 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, съобразно посоченото в чл. 9, ал. 3. Същото следва да бъде подписано от всички членове, участвали в гласуването. В случая заседанието е проведено в присъствието на трима членове, т.е. налице е необходимият кворум, а решението е взето единодушно от всички присъстващи, поради което безспорно е формирано мнозинство и решението е валидно взето. В тази връзка следва да се приемат за неоснователни изложените доводи за липса на компетентност.

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, вр. чл. 59, ал. 2, т. 4 от АПК.
Производството е започнало по подадено на основание чл. 33 от Регламент (ЕС) 2016/679, уведомление за нарушение на сигурността на личните данни, образувана е преписка, събрани са необходимите документи, извършен е анализ на постъпилата информация. След изясняване от фактическа страна, въз основа на извършена проверка, за която дружеството е уведомено и е представило допълнителни доказателства, КЗЛД, на свое заседание е взела решението си, като е издала и изричен писмен акт, в който е изложила съображенията си и крайното си решение.
Жалбоподателят твърди наличието на съществено нарушение на административно производствените правила, тъй като дружеството не е уведомено за проведено на 13.09.2023 г. заседание на комисията, на което е взето оспореното решение, което е довело до лишаване на администратора от възможността да изрази позицията си във връзка с определяне размера на административното наказание, наличието на смекчаващи отговорността обстоятелства и други релевантни факти, имащи значение за индивидуализацията на наказанието. Това твърдение настоящият състав намира за неоснователно поради следното.
Преписката е образувана по подадено уведомление по реда на чл. 33 от Регламента, а реда 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 вр. 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 07.09.2022 г. е взето решение за извършване на проверка на място, за което решение жалбоподателят е уведомен, видно от писмо от 17.02.2023 г., като е уведомен за датата и часа на извършване на проверката и е приканен представител на дружеството да присъства на проверката. За извършената проверка е съставен КА, с рег. № ППН-02-439/06.07.2023 г., в който е отразено, че проверката е извършена в присъствието на представител на дружеството, негов адвокат и преводач. След приключване на проверката, КЗЛД е взела решението си, съгласно чл. 63, ал.3 от Правилника за дейността на КЗЛД, на свое закрито заседание, проведено на 13.09.2023 г., за което е съставен протокол № 30. Както бе посочено, производството по Раздел VII от ППКЗЛДНА е особено производство, като разпоредбите не препращат към производството по реда на Раздел II от ППКЗЛДНА, във вр с чл. 38 от ЗЗЛД, като в настоящия случай комисията постановява решение след провеждане на закрито заседание, без участието на администратора на лични данни.
В допълнение следва се посочи, че съобразно изр. второ на чл. 9, ал. 4 от ЗЗЛД, комисията може да реши отделни заседания да бъдат закрити, което е изключение от общото правило за откритост и публичност на заседанията на КЗЛД.
Решението е издадено при липсата на допуснати нарушения на административнопроизводствените правила, които да бъдат квалифицирани като съществени по смисъла на чл. 146, т. 3 от АПК и да обуславят отмяната му.

Настоящият съдебен състав поддържа мнението, че нарушението на административнопроизводствените правила е съществено само тогава, когато е повлияло или е могло да повлияе върху крайното решение по същество на административния орган.

По съответствие на заповедта с материалния закон:
Настоящият съдебен състав намира, че решението е издадено в съответствие с материалния закон, поради следното. Съдебният контрол за материална законосъобразност на оспореното решение обхваща преценката дали са налице установените от административния орган релевантни юридически факти изложени като мотиви в акта и доколко същите изпълват състава на посоченото в решението правно основание за издаването му.
По делото безспорно се установява, че „Сибериан Уолф“ ЕООД е администратор на лични данни.
Съобразно разпоредбата на чл. 4, § 1 от Регламент /ЕС/ 2016/679 лични са данните за лицето, с които то безспорно може да бъде идентифицирано. Цитираната разпоредба казва, че „лични данни“ означава 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, ал. 2 от регламента, обработване на лични данни 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, § 1 от Регламент 2016/679, личните данни следва да са 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“).

В чл. 5, § 2 от Регламент 2016/679 е регламентиран принципът за отчетност, а именно, 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.

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.

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.

Съгласно посоченото в чл. 5, § 2 от Регламент (ЕС) 2016/679, отговорност на „Сибериан Уолф“ ЕООД е да докаже спазването на принципите за обработване на данни, дефинирани в § 1, посочени по-горе. В настоящия случай, администраторът не е доказал надлежно документиране на всички процеси по обработване на личните данни, не е създал документална среда относно обработването на личните данни, т.е. да разполага с писмени документи, които да позволяват проследимост на процесите по обработване на данните в насока законосъобразно, добросъвестно, прозрачно и в минимален обем за постигане на ясно определените цели, като данните се съхраняват точно и само за времето, необходимо за постигане на тези цели, а посоченото обработване е обезпечено с подходящо ниво на сигурност и защита на данните. По този начин безспорно е реализирано нарушение на „принципа за отчетност“ по чл. 5, § 2 от Регламент (ЕС) 2016/679.

Правилно КЗЛД е приела, че с разпоредбата на чл. 28 от Регламент (ЕС) 2016/679 се вменява задължение на съответния администратор да използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на регламента и да осигурява достатъчна защита на правата на субектите на данни като надеждност и ресурси, че ще предприемат технически и организационни мерки, които отговарят на изискванията на регламента, включително на изискванията за сигурността на обработването. А извършването на обработването от обработващ лични данни следва да се урежда писмено между администратора и обработващия с договор или друг правен акт, като документът следва да регламентира предмета и продължителността на обработването, естеството

и целите на обработването, вида лични данни и категориите субекти на данни, като се вземат предвид конкретните задачи и отговорности на обработващия лични данни в контекста на обработването, което следва да се извърши, както и рискът за правата и свободите на субекта на данни. Именно в писмения документ между администратора и обработващия следва да бъдат разписани клаузи, съгласно които след приключване на обработването от името на администратора, обработващият личните данни да предаде съответните документи.

От доказателствата по делото безспорно се установява, че жалбоподателят не е спазил задължението произтичащо от текста на чл. 28 от Регламент (ЕС) 2016/679, като е възложил чрез устна договорка и при липсата на ясни критерии за избор на изпълнител, който да изработи сайта на дружеството www.wolfintech.com. Не е сключен писмен договор, който ясно н подробно да регулира отношенията между дружеството и изпълнителите, които са разработили сайта www.wolfintech.com, както и да регулира как и на какъв етан дружеството ще има пълен достъп до своя уебсайт. Като не е сключен писмен договор, съответно не са договорени също и отговорността и санкциите спрямо разработчиците на сайта www.wolfintech.com в случай на неизпълнение, включително и по отношение законосъобразността на действията, свързани с обработваните лични данни. По повод с дейността си администраторът е следвало да събира и обработва голям обем от лични данни на своите клиенти, включително такива, с достъпването на които за лицата могат да настъпят сериозни финансови загуби. От дружеството не са оценени рисковете с различна вероятност и тежест за правата и свободите на физическите лица. Именно предвид факта, че не е имало ясни правила и критерии по отношение на техническите и организационни мерки при изработване на интернет страницата, администраторът е допуснал, лицата разработили същата, да имат безконтролен достъп до предоставените данни, като за този период не е могъл да осигури и съответната сигурност и гаранции за законосъобразното обработване на предоставените от клиентите данни. Всичко това се потвърждава и от предоставения доклад на Dracteam Technology LLC, които са извършили проверка и оценка на състоянието на активите на www.wolfintech.com.

Действително, в настоящия случай, засегнати са данни за имена, ЕГН, копие на лична карта, месторождение, телефон, е-мейл, снимка на лицето с цел идентифициране и доказване на идентичност със субекта, чиито паспортни данни са предоставени, чувствителни данни - расов, етнически произход, финансови данни - имотно състояние, финансово състояние, произход на активи. Посредством изброените данни лицата може недвусмислено да бъдат идентифицирани, съответно потенциалното въздействие върху субектите на данни може да доведе до загуба на контрол над личните им данни, също и загуба на поверителност на личните данни на засегнатите субекти. Касае се за не малък брой физически лице, голяма част от тях граждани на Италия и Румъния.

От изложеното може да се направи обоснован извод, че административният орган законосъобразно е приел, че с описаните действия, жалбоподателят е допуснал нарушение на основни принципи при обработването на личните данни, установени в чл. 5, ал. 1, б. „е“, във вр. с чл. 32, § 1, буква „б“ и буква „г“ и чл. 5, § 2 от Регламент /ЕС/ 2016/679, както и на чл. 25, чл. 28 и чл. 32, § 1, буква „б“ и буква „г“от Регламент /ЕС/ 2016/679.

Комисията разполага с оперативна самостоятелност и в съответствие с предоставените й функции преценява кое от корективните правомощия по чл. 58, ал. 2

от Регламент (ЕС) 2016/679 да упражни. Тези правомощия, 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. Предвидените в б. "и" на чл. 58, § 2 "глоба" или "имуществена санкция", имат санкционен характер и се прилага в допълнение. 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. 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 конкретното физическо лице – субект на данни, както и на обществения интерес.
Наложената санкция е законосъобразна, доколкото разпоредбата на чл. 83, ал. 5, б.„а“ от Регламент (ЕС) 2016/679 е санкционна именно за нарушаване на основните принципи на чл. 5 от регламента. Правилно е наложена „имуществена санкция, а не „глоба“, тъй като „Сибериан Уолф“ ООД не е физическо лице и като администратор на лични данни, следва да носи административно-наказателна отговорност „имуществена санкция“. Решението съдържа точни и ясни мотиви за направения избор на най-ефективна, целесъобразна и съответна на принципа на пропорционалност мярка за констатираното нарушение. Изложени са ясни мотиви относно това кои обстоятелства възприема като отегчаващи отговорността и причините за това, т.е. съображения от органа, свързани с тежестта на извършеното нарушение са налице. Видно от характера на засегнатите обществени отношения и предвидените санкции, законодателят е презюмирал 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. Поради това съдът приема за неоснователни доводите на жалбоподателя, че не са обсъдени от органа наличието на смекчаващи отговорността обстоятелства и други релевантни факти, имащи значение за индивидуализацията на наказанието.
Следователно, не е налице твърдяната от жалбоподателя незаконосъобразност. В хода на настоящото производство не се установиха други нарушения на административнопроизводствените правила, които да представляват самостоятелно основание за отмяна на оспореното решение.
Въз основа на изложеното и като провери законосъобразността на оспорения акт по реда на чл. 168 от АПК, съдът приема, че същият е законосъобразен, като издаден в съответствие с процесуалните правила и материалноправните разпоредби. А жалбата като неоснователна, да се отхвърли.

По разноските:
Предвид изхода на спора, на жалбоподателя разноски не се дължат.
Ответникът претендира разноски за юрисконсултско възнаграждение. Предвид изхода на делото, такива му се дължат. При определяне размера на разноските, съдът съобрази разпоредбите на чл. 78, ал. 8 от ГПК, във вр. чл. 37 от Закона за правната помощ и чл. 24 от Наредба за заплащането на правната помощ. В тази връзка, като съобрази фактическа и правна сложност на делото, процесуалната активност на

пълномощника - юрисконсулт при разглеждане на делото, обема и качеството на осъществената процесуална дейност, в полза на ответника следва да се присъдят разноски в размер на 100,00 лв.
Мотивиран от гореизложеното и на основание чл. 172, ал. 2, предложение второ от АПК, Административен съд София-град, II отделение, 59 състав

Р Е Ш И :

ОТХВЪРЛЯ жалбата на „Сибериан Уолф“ ООД, срещу решение № ПАИКД-13-40/2022 от 08.01.2024 г. на Комисията за защита на личните данни.
ОСЪЖДА „Сибериан Уолф“ ООД, с ЕИК[ЕИК], **ДА ЗАПЛАТИ** на Комисия за защита на личните данни сумата от 100,00 лв. направени по делото разноски за юрисконсулско възнаграждение.
РЕШЕНИЕТО подлежи на обжалване с касационна жалба, в 14-дневен срок от съобщаването му на страните пред Върховния административен съд.
Решението да се съобщи на страните чрез изпращане на препис от него по реда на чл. 137 от АПК.

СЪДИЯ: