Анонимизиран текст

Дело C-340/21

Преюдициално запитване

Дата на постъпване в Съда:

2 юни 2021 г.

Запитваща юрисдикция:

Върховен административен съд (България)

Дата на акта за преюдициално запитване:

14 май 2021 г.

Касатор:

VB

Ответник по касационната жалба:

Национална агенция за приходите

ОПРЕДЕЛЕНИЕ

София, 14.05.2021

Върховният административен съд на Република България [OMISSIS]

[OMISSIS]

Производството е по чл. 208 и сл. от Административнопроцесуалния кодекс (АПК).

Административно[то] дело [OMISSIS] е образувано по касационна жалба, подадена от VB[от] гр. София [OMISSIS] против решение [от] [OMISSIS] 27.11.2020 г. [OMISSIS] на Административен съд София-град. С решението е отхвърлен като неоснователен иск против Националната агенция за приходите с цена 1000 (хиляда) лева за претърпени неимуществени вреди с правно основание чл. 82 от Регламент (ЕС) 2016/679 на Европейския

парламент и на Съвета от 27.04.2016 г. 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), чл. 1, ал.1 от Закона за отговорността на държавата и общините за вреди, чл. 203 от Административнопроцесуалния кодекс и чл. 39, ал. 2 от Закона за защита на личните данни.

В хода на произнасяне по съществото на спора Върховният административен съд, [OMISSIS] като взе предвид, че решението по настоящото съдебно производство е окончателно, намира, че за правилното разрешаване на спора е необходимо тълкуване на относими норми на общностното право, за което е необходимо да отправи по своя инициатива запитване до Съда на Европейския съюз по реда на чл. 267, параграф 3 от Договора за функциониране на Европейския съюз за тълкуване на чл. 5, пар. 2, чл. 24, чл. 32, чл. 82, пар. 1 и 3 във връзка със съображения 74, 85 и 146 от Регламент (ЕС) 2016/679.

I. Запитваща юрисдикция

Върховен административен съд на Република България [OMISSIS].

[OMISSIS]

II. Страни по делото

Касатор - VB от гр. София, [OMISSIS].

Ответник по касационната жалба — Националната агенция за приходите (НАП), [OMISSIS].

III. Предмет на главното производство и относими факти.

1. Производството пред Върховния административен съд, [OMISSIS] е касационно.

С касационната жалба VB оспорва решение [от] [OMISSIS] 27.11.2020 г. [OMISSIS] на Административен съд София-град, с което е отхвърлен като неоснователен искът ѝ за присъждане на обезщетение в размер на 1000 лв. за претърпени неимуществени вреди от незаконосъобразно бездействие на ответника Национална агенция за приходите като администратор на лични данни, изразяващо се в неизпълнение в достатъчна степен на задължения по чл. 59, ал.1 от Закона за защита на личните данни, чл. 24 и чл. 32 от Регламент (ЕС) 2016/679, с правно основание чл. 1, ал.1 от Закона за отговорността на държавата и общините за вреди (ЗОДОВ).

2. Пред Административен съд София-град на 16.09.2019 г. са предявени субективно съединени искове на 157 физически лица, [OMISSIS] против

Националната агенция за приходите, с правно основание чл. 82, пар.1 от Регламент (ЕС) 2016/679, чл. 203 от Административно процесуалния кодекс, чл. 1, ал. 1 от Закона за отговорността на държавата и общините за вреди, с искане да бъдат присъдени обезщетения за претърпени неимуществени вреди в размер за всеки от ищците по 1000 (хиляда) лева. С определение от 20.09.2019 г. [OMISSIS] Административен съд София-град (АССГ) съдът е разделил производството, като е образувал отделно дело по иск на всеки от ищците. Искът на VB е образуван в адм.д. № 11217/2019 г. по описа на АССГ.

3. Фактически и правни основания на предявения осъдителен иск:

3.1. На 15.07.2019 г. от медиите е станало известно на цялото общество, че е осъществен неразрешен достъп до информационната система на НАП и е публикувана информация, съдържаща се в информационните бази данни на Агенцията, представляваща лични данни и данъчна и осигурителна информация. Засегнати са 4 057 328 бр. активни български граждани, като общият брой на всички засегнати физически лица е 6 074 140 бр., което включва български и чужди граждани, в това число с прекратена регистрация. Сред засегнатите субекти на данни е ищцата VB.

3.2. Ищцата твърди в исковата молба, че НАП „не е изпълнила в най-добра степен“ задължението си „да обезпечи по безупречен начин своята „киберсигурност“ и „в най-голяма степен да гарантира по ефективен начин сигурността на личните данни на гражданите на Република България“. С това е нарушена сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679 и неправомерно са разкрити лични данни. Наведен е довод, че „неполагането на достатъчна грижа и неприлагане на ефективни мерки за защита на сигурността на данните“ представлява бездействие от страна на НАП да изпълни задълженията си да защити данните на гражданите и представлява нарушение на чл. 24 и чл. 32 от Регламент (ЕС) 2016/679. Като администратор на лични данни НАП трябва да обработва лични данни по начин, който „да гарантира подходящо ниво на сигурност“, като се прилагат подходящи технически и организационни мерки, да се извършва оценка на въздействие на предвидените операции при обработването.

3.3. Ищцата посочва, че вследствие на неизпълнение на задълженията от страна на НАП е претърпяла неимуществени вреди, които се изразяват в притеснения и опасения, че с личните ѝ данни може да бъде злоупотребено в бъдеще, като например че ще бъде отчуждено имуществото ѝ, ще бъде злоупотребено с банковите ѝ сметки или ще бъдат изтеглени кредити от нейно име, може да бъде променено гражданското ѝ състояние или откраднатата самоличността ѝ. Възмутена е от допуснатия „голям пробив в информационната система на НАП“ и се чувства незащитена от държавата. Страхува се да не бъде изнудвана, нападната, отвлечена.

3.4. Претендира обезщетение в размер на 1000 лв. на основание чл. 82, пар. 1 от Регламент (ЕС) 2016/679, чл. 1, ал. 1 от Закона за отговорността на държавата за вреди, чл. 203 от АПК и чл. 39, ал. 1 от Закона за защита на личните данни.

4. Защитната теза на НАП:

4.1. Искът е неоснователен. Ищцата не е поискала информация от НАП какви точно лични данни са достъпени.

4.2. Агенцията веднага е предприела мерки за защита правата и интересите на гражданите. Проведени са срещи с представители и експерти от Дирекция „Документи за самоличност“, Главна дирекция „Национална полиция“, Главна дирекция „Борба с организираната престъпност“, Нотариална камара ([OMISSIS], Агенция по вписванията [OMISSIS], Асоциация на търговските банки, Национално сдружение на общините за обсъждане на възможни рискове и координиране на действия за ограничаване и информиране на гражданите. НАП, Нотариалната камара и Агенцията по вписвания многократно са оповестили, че няма непосредствена опасност за имуществото на гражданите, а председателят на Асоциацията за отговорно небанково кредитиране е дал изявления, че не съществува опасност да се теглят кредити с чужди лични данни и не се налага смяна на документите за самоличност. В сайта на НАП са създадени специални рубрики, свързани с кибератаката на НАП, в които е публикувана актуална информация, [а] експерти отговарят на най-често задаваните въпроси. Всички предприети мерки и ежедневните изявления в средствата за масова информация са извършени с цел успокояване на гражданите.

4.3. Няма причинна връзка между твърдените неимуществени вреди и неоторизирания достъп до лични данни. Самата агенция е обект на злоумишлено посегателство от страна на трети лица, които не са служители на НАП. Затова не следва да носи отговорност за настъпилите вредоносни последици.

4.4. НАП твърди, че е въвела следните мерки:

4.4.1. Система за управление на бизнес процесите и система за управление на сигурността на информацията.

4.4.2. Утвърдените процедури в НАП по чл. 10, ал.1, т. 5 от Закона за Националната агенция за приходите (НАП), са съобразени с международни стандарти за качество ISO 9000 и ISO 9001.

4.4.3. Прилагат се политики, правила, процедури, указания и методики за управление на сигурността на информацията в НАП по отношение на всички защитени данни.

4.[4.4.] Информационни системи на НАП се разработват, тестват и внедряват, съобразно вътрешни процедури.

4.5. Представени са писмени доказателства:

4.5.1. Заповед [от] [OMISSIS] 23.01.2013 г. на Изпълнителния директор на НАП за вида, съдържанието, реда за създаване, поддържане, достъп до регистъра на НАП и база данни за задължените лица, формата и елементите на данъчно-осигурителната сметка.

4.5.2. Заповед на Изпълнителния директор за внедряване на СУСИ по стандарт БДС ISO/IES 27001:2006.

4.5.3. Заповед [от] [OMISSIS]

17.06.2016 г. на Изпълнителния директор за утвърждаване на процедури на отдел „Превенция на финансова и информационна система и вътрешни правила за мрежовата и информационна сигурност“, Политика за информационната сигурност на НАП м. май 2016 г. версия 3.0.

4.5.4. Заповед [от] [OMISSIS] 29.11.2017 г. на Изпълнителния директор за утвърждаване на указания за обозначаване и работа с информация, версия 3.0.

4.5.[5]. Политика по защита на личните данни, утвърдена със заповед [от] [OMISSIS] 25.05.2018 г. на Изпълнителния директор на НАП.

4.5.[6]. Инструкция [OMISSIS] от 8.05.2019 г. за мерките и средствата за защита на лични данни, обработвани от НАП и реда за движение на преписки и заявяване на регистри.

4.5.[7]. Методика за оценка на риска и процедура за оценка на риска.

4.5.[8]. Приключила през 2018 г. проверка от Държавна агенция за електронно управление, в хода на която не са констатирани нарушени[я] на Закона за електронно управление, на Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги, на Наредбата за общите изисквания за мрежова и информационна сигурност.

5. Решението на първоинстанционния съд

5.1. Първоинстанционният съд е определил правното основание на иска по чл. 1, ал.1 от Закона за отговорността на държавата и общините за вреди.

5.2. Съдът е посочил, че неразрешеният достъп до базата данни на НАП е извършен чрез „хакерска атака“ от лица, спрямо които образуваното досъдебно производство не е приключило.

5.3. Престъпният резултат не презюмира неизпълнение на задължения от страна на администратора на данни да приложи подходящи технически и организационни мерки за осигуряване на защитата на базата данни, така че по никакъв начин, от никого и с никакви средства да не може да бъде достъпена.

5.4. В тежест на ищеца е да посочи какви фактически (технически) действия е следвало да извърши НАП или длъжности лица към нея, но не ги е извършила или ги е извършила лошо, така че е настъпил или е допринесено за настъпване на резултата, който се изразява в неразрешен достъп и разкриване на лични данни.

5.5. Не е налице бездействие от администратора на лични данни, предвид представените от него писмени доказателства.

5.6. Ищцата не е претърпяла неимуществени вреди, които да подлежат на обезщетяване. Преживеният емоционален дискомфорт, който предизвиква новината за неоторизиран достъп до информационните масиви на НАП, е нормален, но не представлява реално настъпила вреда по смисъла на закона. Ищцата не е проявила интерес какви точно нейни лични данни са достъпени и това поведение не обосновава силен емоционален стрес.

5.7. Публичното оповестяване на неправомерния достъп до базата данни на НАП не се е отразил върху живота на ищцата — самочувствие, самооценка, работа, отношения с близки хора, здравословно състояние.

5.8. Няма причинно-следствена връзка с преживените негативни емоции, тъй като те не са резултат от поведението на НАП.

6. Оспорване на решението пред Върховния административен съд

6.1. Доводи в касационна жалба на VB пред Върховния административен съд:

6.1.1. Първоинстанционният съд е разпределил неправилно доказателствена[та] тежест за доказване на отрицателен факт, каквото е бездействието на администратора на лични данни да приложи подходящи технически и организационни мерки.

6.1.2. Прилагането на ефективни мерки е в оперативната самостоятелност на НАП, поради което е в невъзможност да опише какви точно конкретни задължения е трябвало да изпълнят служителите на НАП, но не са го направили.

6.1.3. Представените писмени доказателства от НАП за издадени указания, вътрешни правила, методики, политики, инструкции не доказват, че приложените организационни и технически мерки са подходящи.

6.1.4. Притесненията от възможни в бъдеще злоупотреби с лични данни не са хипотетични, а реални неимуществени вреди, които подлежат на обезщетяване. Не е необходимо да представя доказателства за установяване на обичайни неимуществени вреди. Позовава се на решение [от] [OMISSIS] 18.03.2016 г. [OMISSIS] на Върховния касационен съд, постановено по чл. 2 от Закона за отговорността на държавата и общините за вреди, за присъждане на обезщетение за неимуществени вреди от незаконно наказателно преследване и обвинение в извършено престъпление.

6.2. Защитната теза на НАП пред Върховния административен съд.

6.2.1. Доказателствената тежест е правилно разпределена от първоинстанционния съд.

6.2.2. Правилно съдът е приел, че Националната агенция за приходите като администратор на лични данни не е бездействала и е предприела редица технически и организационни мерки за защита при обработването на лични данни, като е представила правила, утвърдени процедури, съобразени и с международни стандарти за мрежовата и информационна сигурност.

6.2.3 Няма доказателства за реално настъпили вреди. Притесненията и страхът за бъдещи събития не следва да се обезщетяват и правилно искът е отхвърлен.

7. Фактическа обстановка по главния спор

7.1. Националната агенция за приходите (НАП) е администратор на лични данни по смисъла на чл. 4, пар. 7 от Регламент(ЕС) 2016/679. Съгласно чл. 2 от Закона за Националната агенция за приходите агенцията е специализиран държавен орган към министъра на финансите за установяване, обезпечаване и събиране на публични вземания и определени със закон частни държавни вземания, и обработва лични данни за изпълнение на възложените ѝ публични функции.

7.2. На 15.07.2019 г. от медиите е станало известно на цялото общество, че е осъществен неразрешен достъп до информационната система на НАП и е публикувана информация, съдържаща се в информационните бази данни на Агенцията, представляваща лични данни и данъчна и осигурителна информация на милиони граждани.

7.3. На основание чл. 33 от Регламент (ЕС) 2016/679 Националната агенция за приходите е уведомила незабавно Комисията за защита на личните данни. Уведомени са и специализирани звена в Държавна агенция „Национална сигурност“, Главна дирекция „Борба с организираната престъпност“ при Министерството на вътрешните работи, Специализираната прокуратура, Държавна агенция „Електронно управление“, възложена е проверка на Инспектората на НАП. От представени по делото публикации в медиите е

видно, че неправомерно достъпената база данни е публикувана в интернет пространството.

7.4. На проведеното изслушване на прокурори от Прокуратурата на Република България на 26.09.2019 г. пред Временната анкетна комисия към Парламента за изясняване на факти и обстоятелства около случая с изтичането на информация от електронната база данни на НАП е посочено, че е образувано досъдебно производство срещу три физически лица, които не са служители на НАП. Не е установено участие на служители на НАП. Засегнати са 4 057 328 бр. активни български граждани, като общият брой на всички засегнати физически лица е 6 074 140 бр., което включва български и чужди граждани, в това число с прекратена регистрация.

7.5. След осъществения достъп до информационната система на НАП на 15.07.2019 г. и публикуване в интернет пространството на информация, съдържаща се в информационните бази данни на Агенцията, са заведени стотици дела от граждани срещу Националната агенция за приходите за присъждане на обезщетение за неимуществени вреди.

7.6. До настоящия момент няма влязла в сила присъда срещу лицата, които са извършили неоторизирания достъп, наречен в средствата за масово осведомяване „хакерска атака“.

7.8. С решение [от] [OMISSIS] 22.08.2019 г. на Комисията за защита на лични данни на Националната агенция за приходите са дадени предписания да предприеме подходящи технически и организационни мерки с цел повишаване защитата при обработване на лични данни в приложения за електронни услуги към гражданите. Решението е оспорено пред Административен съд София-град като първа съдебна инстанция, делото е висящо и не е приключило с влязъл в сила съдебен акт.

7.9. С наказателно постановление [от] [OMISSIS] 28.08.2019 г. на председателя на Комисията за защита на лични данни на Националната агенция за приходите е наложена имуществена санкция за неизпълнение на задълженията по Регламент (ЕС) 2016/679 и неприлагане на подходящи технически и организационни мерки, в резултат на което е осъществен неразрешен достъп, неразрешено разкриване и разпространяване на лични данни на физически лица от информационните бази данни, поддържани от Националната агенция за приходите. Наказателното постановление също е обжалвано пред съд и към настоящия момент няма влязло в сила съдебно решение.

7.10. При извършена справка чрез SMS чрез специално разработения софтуер за справки от интернет портала на НАП ищцата е разбрала, че е сред гражданите, на които личните данни са неправомерно разкрити. Не е установено конкретно какви лични данни на ищцата са достъпени.

7.11. До приключване на делото няма твърдение и данни да е извършена злоупотреба с личните данни на VB.

7.12. Разпитаният от съда свидетел посочва, че ищцата е изпитвала притеснения, че трети лица са осъществили достъп до личните ѝ данни.

IV. Приложимо национално право

1. Административнопроцесуален кодекс

[OMISSIS]

Глава единадесета

ПРОИЗВОДСТВА ЗА ОБЕЗЩЕТЕНИЯ

Приложим закон

Чл. 203. (1) [OMISSIS] Исковете за обезщетения за вреди, причинени на граждани или юридически лица от незаконосъобразни актове, действия или бездействия на административни органи и длъжностни лица, се разглеждат по реда на тази глава.

(2) [OMISSIS] За неуредените въпроси за имуществената отговорност по ал. 1 се прилагат разпоредбите на Закона за отговорността на държавата и общините за вреди или на Закона за изпълнение на наказанията и задържането под стража.

2. Граждански процесуален кодекс

Доказателствена тежест

Чл. 154. (1) Всяка страна е длъжна да установи фактите, на които основава своите искания или възражения.

(2) Не е необходимо да се доказват факти, за които съществува установено от закон предположение. Оборване на такива предположения се допуска във всички случаи, освен когато закон забранява това.

3. Закон за отговорността на държавата и общините за вреди

Отговорност за дейност на администрацията

Чл. 1. [OMISSIS] (1) (Доп. — ДВ, бр. 94 от 2019 г.) Държавата и общините отговарят за вредите, причинени на граждани и юридически лица от незаконосъобразни актове, действия или бездействия на техни органи и длъжностни лица при или по повод изпълнение на административна дейност, както и за вредите, причинени от действието на отменени като

незаконосъобразни или обявени за нищожни подзаконови нормативни актове.

(2) [OMISSIS] Исковете по ал. 1 се разглеждат по реда, установен в Административнопроцесуалния кодекс, като местната подсъдност се определя по чл. 7, ал. 1.

Редакция към 15.07.2019 г.[:]

Отговорност за дейност на администрацията

Чл. 1. [OMISSIS] (1) Държавата и общините отговарят за вредите, причинени на граждани и юридически лица от незаконосъобразни актове, действия или бездействия на техни органи и длъжностни лица при или по повод изпълнение на административна дейност.

(2) Исковете по ал. 1 се разглеждат по реда, установен в Административнопроцесуалния кодекс, като местната подсъдност се определя по чл. 7, ал. 1.

V. Приложимо право на Съюза

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

(74) Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-специално, администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с настоящия регламент, включително ефективността на мерките. Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица.

(76) Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до риск или до висок риск.

(77) Насоки за прилагането на подходящи мерки и за доказване на съответствие от страна на администратора или обработващия лични данни, особено по отношение на идентифицирането на риска, свързан с обработването, оценката по отношение на произход, естество, вероятност и

тежест и определянето на добри практики за ограничаване на риска, биха могли да се предоставят по-специално чрез одобрени кодекси на поведение, одобрени механизми за сертифициране, насоки на Комитета или чрез указания, предоставени от длъжностното лице за защита на данните. Комитетът може също да издава насоки относно операции по обработване, за които се счита, че е малко вероятно да доведат до висок риск за правата и свободите на физическите лица, и да даде указания какви мерки могат да бъдат достатъчни в такива случаи за преодоляването на такъв риск.

(83) 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.

(85) Нарушаването на сигурността на лични данни **може**, ако не бъде овладяно по подходящ и навременен начин, **да доведе до физически, материални или нематериални вреди за физическите лица, като** загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица. Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми надзорния орган за нарушението 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, освен ако администраторът не е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и че информацията може да се подаде поетапно без ненужно допълнително забавяне.

146) Администраторът или обработващият лични данни следва **да обезщетят всички вреди, които дадено лице може да претърпи в**

резултат на обработване на данни, което нарушава настоящия регламент. Администраторът или обработващият лични данни следва да бъде **освободен от отговорност, ако докаже, че по никакъв начин не е отговорен за вредите. Понятието „вреда“ следва да се тълкува в по-широк смисъл в контекста на съдебната практика на Съда по начин, който отразява напълно целите на настоящия регламент**. Това не засяга евентуални искове за вреди, произтичащи от нарушаване на други правила на правото на Съюза или правото на държава членка. Обработване на данни, което нарушава настоящия регламент, включва и обработване, което нарушава делегираните актове и актовете за изпълнение, приети в съответствие с настоящия регламент, и правото на държава членка, конкретизиращо правилата на настоящия регламент. **Субектите на данни следва да получат пълно и действително обезщетение за претърпените от тях вреди** […].

Член 4

Определения

2) „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

12) „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

Член 5

Принципи, свързани с обработването на лични данни

2. Администраторът носи отговорност и е в състояние да докаже спазването на параграф 1 („отчетност“).

Член 24

Отговорност на администратора

1. Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия

регламент. Тези мерки се преразглеждат и при необходимост се актуализират.

2. Когато това е пропорционално на дейностите по обработване, посочените в параграф 1 мерки включват прилагане от страна на администратора на подходящи политики за защита на данните.

3. Придържането към одобрени кодекси за поведение, посочени в член 40[,] или одобрени механизми за сертифициране, посочени в член 42[,] може да се използва като елемент за доказване на спазването на задълженията на администратора.

Член 32

Сигурност на обработването

1. 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 с оглед да се гарантира сигурността на обработването.

2. 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.

3. Придържането към одобрен кодекс за поведение, посочен в член 40 или одобрен механизъм за сертифициране, посочен в член 42 може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграф 1 от настоящия член.

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.

Член 82

Право на обезщетение и отговорност за причинени вреди

1. Всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди.

2. Администраторът, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава настоящия регламент. Обработващият лични данни носи отговорност за вреди, произтичащи от извършеното обработване, само когато не е изпълнил задълженията по настоящия регламент, конкретно насочени към обработващите лични данни, или когато е действал извън законосъобразните указания на администратора или в противоречие с тях.

3. Администраторът или обработващият лични данни се освобождава от отговорност съгласно параграф 2, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

4. Когато в една и съща операция по обработване участват повече от един администратор или обработващ лични данни или участват и администратор, и обработващ лични данни, и когато те са отговорни по параграфи 2 и 3 за вреда, причинена от обработването, всеки администратор или обработващ лични данни носи отговорност за цялата вреда, за да се гарантира действително обезщетение на субекта на данни.

5. Когато администратор или обработващ лични данни е изплатил съгласно параграф 4 пълното обезщетение за причинената вреда, той има право да поиска от другите администратори или обработващи лични данни, участвали в същата операция по обработване на лични данни, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда в съответствие с условията по параграф 2.

6. Съдебните производства във връзка с упражняването на правото на обезщетение се образуват пред съдилища, компетентни съгласно правото на държавата членка, посочена в член 79, параграф 2.

VI. Съдебна практика

1. На националните съдилища

1.1. Тъй като искът е предявен срещу администратор на лични данни, който е орган на изпълнителната власт, националният процесуален ред за защита е по чл. 203 и сл. от Административнопроцесуалния кодекс пред административните, а не пред общите съдилища в страната.

1.2. Една част от образуваните съдебни производства в Република България бяха прекратени от първоинстанционните съдилища с мотиви, че исковете са недопустими, тъй като съществувал специален ред за защита по чл. 39 от Закона за защита на личните данни. Прекратителните определения бяха отменени от Върховния административен съд, а делата върнати за продължаване на съдопроизводствените действия с мотив, че предварителната защита на правата на субекта на лични данни по регламента и по закона по реда на чл. 39, ал. 1 от ЗЗЛД не е процесуална предпоставка за разглеждане на иск с правно основание чл. 82 от Регламент (ЕС) 2016/679. Разпоредбата на чл. 39, ал. 1 от ЗЗЛД съответства на чл. 79 от Регламент (ЕС) 2016/679.

1.3. Съдебните производства срещу НАП са приключили на първа инстанция с противоречиви резултати. Исковете или са отхвърляни като неоснователни или са уважавани изцяло или частично. Нормативната уредба е тълкувана и прилагана противоречиво по всички елементи на отговорността на администратора на лични данни.

1.4. Към настоящия момент са налице влезли в сила следните осъдителни решения по идентични казуси: № 4981/25.09.2020 г. [OMISSIS] на Административен съд София-град, оставено в сила с решение [от] [OMISSIS] 10.05.2021 г. [OMISSIS] на Върховния административен съд, [OMISSIS] решение № 4978/25.09.2020 г. [OMISSIS] на Административен съд София-град, оставено в сила с решение [от] [OMISSIS] 11.05.2021 г. [OMISSIS] на ВАС, [OMISSIS]. С решени[я от] [OMISSIS] 11.05.2021 г. [OMISSIS], [OMISSIS] 1 2.05.2021 г. [OMISSIS] и [OMISSIS] 13.05.2021 г. [OMISSIS] на ВАС, [OMISSIS] [по три други дела] са отменени първоинстанционните решения изцяло или частично, като вместо това са присъдени обезщетения в размери по 200, 300 и 940 лв.

Върховният административен съд приема, че НАП е бездействал[а], не е изпълнил[а] задълженията си по чл. 24 и чл. 32 от Регламент (ЕС) 2016/679 и не е доказал[а], че е въвел[а] подходящи технически мерки, които трябва да осигурят подходящо ниво на сигурност. Безспорно установеният факт на изтекла информация от информационната система на НАП вследствие на неправомерен достъп обуславя извод за бездействие от страна на агенцията да осигури надеждност и сигурност на личните данни. Прието е, че деянието на лицето, проникнало в информационната система на НАП, не освобождава администратора на лични данни от отговорност за вреди по чл. 82, пар. 3 от Регламент (ЕС) 2016/679, доколкото не е ангажирал доказателства, че е взел

изискуемите се по регламента подходящи технически мерки, които да гарантират сигурността на съдържащите се в информационната му система лични данни. Изпитаните от субекта на лични данни негативни емоции, притеснения, страх, несигурност са в причинна връзка с поведението на администратора на лични данни [OMISSIS] представляват реално претърпени неимуществени вреди, свързани с реален страх от реална заплаха за увреждане.

2. Практика на Съда на Европейския съюз

2.1. В Решение на съда (трети състав), 30 май 2013 година по дело C-342/12 Worten - Equipamentos para o Lar SA, ECLI:EU:C:2013:355, т. 24 се посочва, че съгласно член 17, параграф 1 от Директива 95/46, свързан с надеждността на обработването, държавите членки предвиждат, че администраторът на лични данни трябва да прилага технически и организационни мерки, **предназначени да осигурят подходящо равнище на сигурност с оглед рисковете, свързани с обработването и с естеството на данните, които следва да бъдат защитени, като се има предвид съвременното равнище на развитие и разходите за осъществяването им** [OMISSIS]. Спорът в главното производство обаче е за съответствие с директивата на национална разпоредба, която задължава работодател да предостави регистър на работно време като „лични данни“ на разположение на компетентния национален орган за контрол на условията на труд, като в т. 26 от решението изрично е посочено, че от запитването по никакъв начин не се установява, че разглежданите по главното производство данни са били обект на случайно или неправомерно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп, нито на други незаконни форми на обработка по смисъла на член 17, параграф 1 от Директива 95/46. Напротив, от сведенията по преписката, с която разполага Съдът по това дело, е безспорно, че достъпът на компетентните национални органи в областта на контрола на условията на труд до тези данни е разрешен от националното право.

Засега друга практика, относима за решаването на делото, не беше открита.

2.2. При извършена от съдебния състав служебна проверка и сравнително-правен анализ, настоящият състав се запозна със съдебно решение на Oberlandesgerichts Dresden от 11 юни 2019 г. по дело 4 U 760/19, в което [се] приема, че чл. 82 от Регламент (ЕС) 2016/679 не трябва да се тълкува в смисъл, че всяко неприятно усещане (от слаб интензитет), преживяно от засегнатото лице, дава право на обезщетение за претърпяна неимуществена вреда, без да е било предварително установено увреждане на имиджа или на репутацията на лицето.

VII. Връзка с правото на Европейския съюз.

1. В Съображения 1 и 4 от преамбюла на Регламент (ЕС) 2016/679 е посочено, че защитата на физическите лица във връзка с обработването на

лични данни е основно право. Член 8, параграф 1 от Хартата на основните права на Европейския съюз („Хартата“) и член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС) предвиждат, че всеки има право на защита на личните му данни. Правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност. Основанието на предявеният иск за присъждане на обезщетение за претърпени неимуществени вреди в резултат на нарушение на Регламент (ЕС) 2016/679 е чл. 82 от същия. Правната норма регламентира правото на обезщетение и отговорността за причинени вреди. Предвид чл. 288 от Договора за Европейския съюз, регламентът е акт с общо приложение и като такъв се прилага пряко във всички държави членки. Администраторът, участващ в обработването на лични данни по смисъла на чл. 4, т. 2 от Регламент (ЕС) 2016/679, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава настоящия регламент. Прякото прилагане на чл. 82 от Регламент (ЕС) 2016/679 [и] тълкуването на разпоредби от регламента, посочени в настоящото преюдициално запитване, имат значение за изхода [на разглеждания] съдебен спор.

2. В настоящия спор несъмнено е налице необходимост от тълкуване на разпоредбите на чл. 24, чл. 32 и чл. 82, пар. 3 от Регламент 2016/679, което да изясни правилното прилагане на правото на ЕС, в хипотеза като настоящата, за ангажиране отговорността на администратора на лични данни, отделните аспекти и практически проявления на използвания в регламента термин „подходящи технически и организационни мерки“, както и на понятието „нематериални вреди“, подлежащи на обезщетяване в случаи на допуснати нарушения на Регламент (ЕС) 2016/679.

VIII. Мотиви за необходимостта да бъдат отправени преюдициални въпроси.

1. Фактическият състав на отговорността по чл. 82 от Регламент (ЕС) 2016/679 включва следните предпоставки:

1.1. да е налице нарушение на Регламент (ЕС) 2016/679 от администратора на лични данни (респективно от обработващия данни),

1.2. субектът на данни да е претърпял материални или нематериални вреди,

1.3. претърпяната вреда да е резултат от нарушението на Регламент (ЕС) 2016/679, т.е. да е налице причинна връзка.

2. Администраторът на лични данни се освобождава от отговорност, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата — чл. 82, пар. 3 от Регламент (ЕС) 2016/679, което тълкуваме в смисъл, че не е могъл по никакъв начин да предотврати събитието, довело до вредата.

3. Националната агенция за приходите е специализиран държавен орган към министъра на финансите за установяване, обезпечаване и събиране на публични вземания, и определени със закон частни държавни вземания, и обработва лични данни за изпълнение на възложените ѝ публични функции и обработва лични данни на законно основание.

4. Касационната жалбоподателка твърди нарушения на задълженията на администратора по чл. 24 и чл. 32 от Регламент (ЕС) 2016/679 да защити обработването на личните данни на физически лица с подходящи технически и организационни мерки, като в резултат на бездействие е нарушена сигурността на личните данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679 и на принципа за „цялостност и поверителност“ по смисъла на чл. 5, пар.1, б. „е“.

5. Настоящият съдебен състав формулира следните правни проблеми при тълкуване на общностното право, които са релевантни за правилното решаване на спора.

5.1.1. Съгласно чл. 24, пар. 1 от Регламент (ЕС) 2016/679 администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират. За да се изпълни това задължение, администраторът следва да вземе предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица. В съображение 83 от Регламент (ЕС) 2016/679 е пояснено, 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.

5.1.2. С чл. 32 от Регламент (ЕС) 2016/679 са предвидени задължения на администратора във връзка със сигурността на обработването, които са свързани с отговорността му по чл. 24 и я развиват, като [се] посочват **критериите**, по които следва да се прилагат подходящите технически и организационни мерки за осигуряване на съобразено с риска ниво на сигурност. Това са **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.**

5.1.3. Регламентът няма определение за „подходящи технически и организационни мерки“. В съображение 74 е посочено, че администраторът е длъжен да прилага **подходящи и ефективни** мерки и да е в състояние да докаже, че дейностите по обработване са в съответствие с настоящия регламент, включително ефективността на мерките. Мерките следва да

отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица. Администраторът на лични данни има задължението да прилага подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително inter alia, когато е целесъобразно прилага мерки като псевдонимизация и криптиране на лични данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите на обработване, процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационни мерки с оглед да се гарантира сигурността на обработването. Мерките са изброени примерно.

5.1.4. Изложеното налага извод, че администраторът на лични данни трябва да извърши оценка на риска по определените в чл. 32 от Регламент (ЕС) 2016/679 критерии, въз основа на които следва да приложи технически и организационни мерки, които са подходящи с оглед изискуемото според нивото на риска ниво на сигурност на личните данни. С въвеждането на подходящи и технически организационни мерки администраторът на лични данни гарантира по чл. 24 от Регламент (ЕС) 2016/679, че извършва обработването на лични данни в съответствие с регламента.

5.1.5. Цитираната правна уредба насочва към извод, че **изборът на подходящите и технически организационни мерки е въпрос на целесъобразност. Преценката на администратора на лични данни по целесъобразност обаче не е предмет на съдебен контрол, защото съдът осъществява проверка за законосъобразност**. В същото време обработването на лични данни при условията на оперативна самостоятелност в избора на техническите и организационни мерки, следва да става в рамката на регламента и при спазване [на] целта да бъде защитено основното право на защита на лични данни на физическите лица.

5.1.6. В съображени[е] 6 от преамбюла на Регламент (ЕС) 2016/679 законодателят е посочил, че глобализацията и бързото технологично развитие създават нови предизвикателства пред защитата на личните данни поради значителното нарастване на мащаба на обмена, събирането на лични данни и наличието на технологии, които позволяват използване на лични данни в безпрецедентни мащаби.

5.1.7. Именно отчетеното бързо технологично развитие и разходите за прилагане на съответни технически мерки са обективната причина, поради която в определен момент техническите и организационни мерки могат да са подходящи, а в следващия момент да се окажат неподходящи. В случая личните данни са достъпени и разкрити чрез неразрешен достъп от трети лица, които не са служители на НАП и не са действали под неин контрол.

5.1.8. При наличието на задължения за администратора на лични данни по регламента, [а и като се има предвид] предметът на проверка от страна на

съда за законосъобразност, а не за целесъобразност, за настоящия съдебен състав стои въпрос[а] дали разпоредбите на чл. 24 и чл. 32 от Регламент (ЕС) 2016/679 могат да се тълкуват в смисъл, че настъпването на противоправен резултат като неразрешено разкриване или достъп до лични данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679 доказва, че приложените от администратора на лични данни технически и организационни мерки не са били подходящи?

5.2.1. При условие че отговорът на първия поставен въпрос е отрицателен, възниква следващият въпрос, относим към предмета на спора, когато в исковото производство съдът проверява дали администраторът на лични данни е спазил задълженията си по чл. 24 и чл. 32 от Регламент (ЕС) 2016/679.

5.2.2. След като изборът и прилагането на технически и организационни мерки е **предоставен на субективната преценка на администратора на личните данни и е в неговата оперативната самостоятелност**, какъв трябва да е предметът и обхватът на съдебния контрол за законосъобразност при проверка дали приложените от администратора на лични данни технически и организационни мерки са подходящи и съответни на чл. 24 и чл. 32 от Регламент (ЕС) 2016/679?

5.2.3. **Достатъчно ли е съдът да установи по какъв начин администраторът на лични данни е изпълнил произтичащите от двете разпоредби задължения или трябва да изследва по същество въведените и приложени технически и организационни мерки, които в същото време са посочени само примерно в регламента и въвеждането им става по целесъобразност?**

5.2.4. Съгласно чл. 5, пар. 2 от Регламент (ЕС) 2016/679 администраторът *носи отговорност* и следва да е в състояние да докаже спазването на принципите, свързани с обработването на лични данни по чл. 5, пар. 1 от Регламент (ЕС) 2016/679. С чл. 24, пар.1 от Регламент (ЕС) 2016/679 се изисква от администратора на лични данни **да въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже**, че обработването се извършва в съответствие с регламента.

5.2.5. Предвид изложеното и в случай, че отговорът на първия въпрос е отрицателен, какъв следва да е предметът и обхватът на съдебния контрол за законосъобразност при проверка дали приложените от администратора на лични данни технически и организационни мерки по чл. 32 от Регламент (ЕС) 2016/679 са подходящи?

5.3.1. Разпоредбата на чл. 82, пар. 3 от Регламент (ЕС) 2016/679 дава възможност на администратора или обработващия лични данни да се освободи от отговорност, съгласно пар. 2, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата. Параграф 2 вменява

отговорност за администратора на лични данни за вреди, произтичащи от извършеното обработване, което нарушава настоящия регламент.

5.3.2. Съгласно разпоредбата на чл. 154, ал.1 от Гражданскопроцесуалния кодекс, към който препраща разпоредбата на чл. 144, ал.1 от Административнопроцесуалния кодекс, в исковото производство всяка страна е длъжна да установи фактите, на които основава своите искания или възражения.

Първоинстанционните съдилища са разпределяли доказателствената тежест между ищеца и ответника по различен начин.

5.3.3. Принципно тежестта на доказване се урежда от процесуалния закон на съответната държава — членка на ЕС. В случая обаче за правилното прилагане на общностното право е релевантен въпросът дали принципът на отчетност по чл. 5, пар. 2 във връзка със съображение 74 от преамбюла и чл. 24, пар.1 от Регламент (ЕС) 2016/679 могат да се тълкуват в смисъл, че разместват тежестта на доказване и администраторът на лични данни, срещу който е заведен иск за ангажиране на отговорност за претърпени вреди от нарушение на регламента, е длъжен като ответник да доказва, че приложените от него технически и организационни мерки са подходящи?

5.3.4. Освен предмета и обхвата на съдебната проверка за спазване на задълженията по регламента, проблем е как, с какви доказателствени средства трябва да се извърши проверката за тяхното спазване, и по-специално дали са приложени всички **подходящи технически и организационни [мерки]**.

5.3.5. По делото са приложени писмени доказателства от страна на НАП за осигурена защита на информационните мрежи при посочени в документите стандарти, но не е назначавана съдебна техническа експертиза, която да установи дали техническите и организационни мерки са били подходящи по смисъла на регламента. Запитващата юрисдикция е наясно, че такъв администратор на лични данни, какъвто е Националната агенция за приходите, е задължен да прилага организационни, технологични и технически мерки за мрежова и информационна сигурност, които да са пропорционални на заплахите от киберпрестъпността, с цел да минимализира риска от тяхното реализиране. Достъпът обаче на съдебни експерти по всяко дело с правно основание чл. 82 от Регламент (ЕС) 2016/679 би могло да има нови неблагоприятни последици за защитата на лични данни.

5.3.6. Предвид техническия прогрес, съществуващите стандарти за защита за информационните мрежови системи [и] извършения[...] неразрешен достъп чрез „хакерска атака“ от лица, извън администрацията на администратора на лични данни, назначаването на съдебна техническа експертиза от съда може ли да се приеме като необходимо и достатъчно доказателствено средство, с

което да се установи дали въведените и приложени технически и организационни мерки са били подходящи, за да осигурят защитата на личните данни?

5.4.1. Националната агенция за приходите като администратор, участващ в обработването на лични данни по чл. 82, пар. 2 от Регламент (ЕС) 2016/679 носи отговорност, но може да се освободи по пар. 3, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

5.4.2. Няма спор по делото, че личните данни са достъпени чрез „хакерска атака“ от трети лица, които не са служители на НАП, а неразрешеният достъп и разкриване на лични данни не е извършено при и по повод обработване на лични данни от страна на служители на НАП.

5.4.3. Предвид изложеното, може ли разпоредбата на чл. 82, пар. 3 от Регламент (ЕС) 2016/679 да се тълкува в смисъл, че при осъществено неразрешено разкриване или достъп до лични данни по смисъла на чл. 4, т. 12 от Регламент (ЕС) 2016/679 чрез „хакерска атака“ от лица, които не са служители в администрацията на администратора на лични данни и не са под негов контрол, администраторът на лични данни се освобождава от отговорност, защото е събитие, за което по никакъв начин не е отговорен?

5.5.1. Субектът на лични данни претендира обезщетение за неимуществени вреди, които се изразяват в притеснения, страх, стрес, усещане за несигурност, опасения, че с личните ѝ данни ще бъде злоупотребено в бъдеще по различни начини, описани от нея. Няма данни да е извършена злоупотреба с личните данни на ищцата.

5.5.2. Видно от съображения 75 и 85 в Регламент (ЕС) 2016/679, при очертаването на примери за материални или нематериални вреди, които могат да претърпят субектите на данни, се отчитат естеството на личните данни и неблагоприятните последици за субектите на данни, а не само неговите вътрешни преживявания.

5.5.3. Съображение 146 от преамбюла на регламента очертава границата на отговорността и това са „всички вреди“, които дадено лице може да претърпи в резултат на обработване на данни, което нарушава регламента. Понятието „вреда[“] следва да се тълкува в по-широк смисъл в контекста на съдебната практика на Съда по начин, който отразява напълно целите на настоящия регламент“. Субектите на данни следва да получат „пълно и действително“ обезщетение за претърпените вреди.

5.5.4. Веднъж достъпени, личните данни на субекта на данни могат да бъдат обект на редица злоупотреби от неимуществен и имуществен характер, които да са със значителни последици. В обществото са известни случаи на такива злоупотреби, което може да обоснове по-висока степен на безпокойство на засегнатите лица от извършената „хакерска атака“. В случая и предвид липсата на данни за вече осъществена злоупотреба, бъдеща

злоупотреба е само предположение, хипотеза, с вероятен, но несигурен риск за правата на субекта на личните данни.

5.5.5. Изложеното поставя въпрос дали емоционалните негативни преживявания на субекта на лични данни, достъпени чрез неразрешен достъп в хипотеза като настоящата, т.е. самият факт на поставянето им в опасност от евентуална неправомерна употреба, попада в широкия смисъл на понятието нематериални вреди и е основание за обезщетение по чл. 82, ал.1 във връзка със съображение 146 от Регламент (ЕС) 2016/679?

5.5.6. Или правната норма на чл. 82, ал.1 във връзка със съображение 146 от Регламент (ЕС) 2016/679 не може да се тълкува в смисъл, че всяко негативно преживяване, страх, притеснение, претърпяно от засегнатото лице, дава право на обезщетение за претърпяна неимуществена вреда, без предварително да е настъпило неправомерна употреба като отчуждаване на имущество, изтегляне на кредити от името на субекта на лични данни, кражба на самоличност.

5.5.7. Различно е тълкуването на понятието „неимуществени вреди“ като основание за отговорност на администратора на лични данни в съдебните актове на административните съдилища. В една група съдебни решения се приема, че душевните страдания и психически стрес, притеснения и опасения от евентуална бъдеща злоупотреба с лични данни са основание за присъждане на обезщетение, ако са доказани. В други решения (като съдебния акт по настоящото дело) се приема, че такива притеснения и стрес, подлежат на обезщетяване само ако са довели до промяна в начина на живот на ищеца. В трета група решения е посочено, че ищецът се обезщетява и без да е доказал неимуществени вреди като описаните в исковата молба. Има четвърта група решения, в които се приема, че само страхът и притесненията от евентуални бъдещи злоупотреби с лични данни не подлежи на обезщетяване, тъй като не са реални вреди в правната сфера на ищеца.

5.5.8. В цитираните по-горе решения на Върховния административен съд се приема, че само неприятните емоции за възможни, бъдещи злоупотреби с лични данни са неимуществени вреди, които следва да бъдат обезщетени.

5.5.9. По изложените съображения запитващата юрисдикция намира, че следва да бъде зададен въпрос дали нормите на чл. 82, пар. 1 и пар. 2 във връзка със съображения 85 и 146 от преамбюла на Регламент (ЕС) 2016/679 могат да се тълкуват в смисъл, че в хипотеза като настоящата на нарушение на сигурността на личните данни, изразяващо се в неразрешен достъп и разпространение на лични данни, осъществено чрез „хакерска атака“, само преживените от субекта на лични данни опасения, притеснения и страх от евентуална, бъдеща злоупотреба с лични данни, без да е установена такава злоупотреба и/или да настъпила друга вреда за субекта на данните, попадат в широкия смисъл на понятието нематериални вреди и е основание за обезщетение?

5.5.10. В този смисъл правният спор попада изцяло в приложното поле на правото на Съюза, а неизчерпателната уредба на отделни правни институти в режима на отговорността обуславя необходимостта от постановяване на преюдициално запитване.

По изложените съображения и за да постанови решението си в съответствие с приложимите норми от вторичното право на Европейския съюз и с оглед конкретиката на настоящия казус, Върховният административен съд, [OMISSIS] намира за правилно да направи преюдициално запитване до Съда на Европейския съюз с молба за тълкуване на чл. 5, пар. 2, чл. 24, чл. 32, чл. 82, пар. 1, 2 и 3 във връзка със съображения 74, 85 и 146 от Регламент (ЕС) 2016/679.

По изложените съображения Върховният административен съд, [OMISSIS]

ОПРЕДЕЛИ:

[OMISSIS]

ОТПРАВЯ преюдициално запитване до Съда на Европейския съюз съгласно член 267, първи параграф, буква „б“ от Договора за функционирането на Европейския съюз със следните въпроси:

1. Разпоредбите на член 24 и член 32 от Регламент (ЕС) 2016/679 могат ли да се тълкуват в смисъл, че е достатъчно да е осъществено неразрешено разкриване или достъп до лични данни по смисъла на член 4, точка 12 от Регламент (ЕС) 2016/679 от лица, които не са служители в администрацията на администратора на лични данни и не са под негов контрол, за да се приеме, че приложените технически и организационни мерки не са подходящи?

2. Ако отговорът на първия въпрос е отрицателен, какъв следва да е предметът и обхватът на съдебния контрол за законосъобразност при проверка дали приложените от администратора на лични данни технически и организационни мерки по член 32 от Регламент (ЕС) 2016/679 са подходящи?

3. Ако отговорът на първия въпрос е отрицателен, принципът на отчетност в член 5, параграф 2 и член 24 във връзка със съображение 74 от Регламент (ЕС) 2016/679 могат ли да се тълкуват в смисъл, че в исковото производство по член 82, параграф 1 от Регламент (ЕС) 2016/679 администраторът на лични данни носи доказателствена тежест относно обстоятелството, че приложените по член 32 от регламента технически и организационни мерки са подходящи? Назначаването на съдебна експертиза може ли да се приеме като необходимо и достатъчно доказателствено средство, с което да се установи дали приложените от администратора на лични данни технически и организационни мерки са подходящи в хипотеза

като настоящата, в която неразрешеният достъп и разкриване на лични данни е резултат от „хакерска атака“?

4. Нормата на член 82, параграф 3 от Регламент (ЕС) 2016/679 може ли да се тълкува в смисъл, че неразрешено разкриване или достъп до лични данни по смисъла на член 4, точка 12 от Регламент (ЕС) 2016/679, в случая чрез „хакерска атака“, от лица, които не са служители в администрацията на администратора на лични данни и не са под негов контрол, е събитие, за което администраторът на лични данни по никакъв начин не е отговорен и е основание за освобождаване от отговорност?

5. Нормите на член 82, параграф 1 и параграф 2 във връзка със съображения 85 и 146 от преамбюла на Регламент (ЕС) 2016/679 могат ли да се тълкуват в смисъл, че в хипотеза като настоящата на нарушение на сигурността на личните данни, изразяващо се в неразрешен достъп и разпространение на лични данни, осъществено чрез „хакерска атака“, само преживените от субекта на лични данни опасения, притеснения и страх от евентуална, бъдеща злоупотреба с лични данни, без да е установена такава злоупотреба и/или да е настъпила друга вреда за субекта на данните, попадат в широкия смисъл на понятието нематериални вреди и [това] е основание за обезщетение?

СПИРА [OMISSIS] производството по делото до произнасянето на Съда на Европейския съюз.

[OMISSIS]