Р Е Ш Е Н И Е
№ 565

гр. София, 02.02.2023 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 23 състав,** в публично заседание на 19.09.2022 г. в следния състав:

СЪДИЯ: Антоанета Аргирова

при участието на секретаря Емилия Митова, като разгледа дело номер **10477** по описа за **2019** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл. 145 и сл. от Административно-процесуалния кодекс (АПК), вр. чл.38, ал. 7, вр. ал.3 от Закона за защита на личните данни (ЗЗЛД) и чл. 58, § 2, буква „г“ във връзка с чл. 57, § 1, буква „а“ и чл. 83, § 2, букви „а“, „в“, „г“, „е“ и „ж“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

Образувано е по жалба на Националната агенция за приходите (НАП), ЕИК[ЕИК] срещу Решение №ППН-02-399 от 22.08.2019 г., издадено от Председателя на Комисията за защита личните данни /КЗЛД/, с искане да бъде изцяло отменено.

С оспореното административно решение, на основание чл. 58, § 2, буква „г“ във връзка с чл. 57, § 1, буква „а“ и чл. 83, § 2, букви „а“, „в“, „г“, „е“ и „ж“ от Регламент (ЕС) 2016/679 се разпорежда на НАП като администратор на лични данни да съобрази операциите по обработването на данни, както следва:

1. Да изготви ясно разписани правила за отделните потребители в информационните системи на НАП /собственици на данни, разработчици, системни администратори, бизнес анализатори, администратори на бази данни, администратори на приложенията и органи по сигурността данните/, функционалните им задължения и процедурите за тяхната дейност, като дефинира принципите на взаимодействие на отделните потребители. Да изготви процедури за взаимодействие на отделните потребители в

системата за защита на личните данни.

2. Да предприеме подходящи технически и организационни мерки с цел повишаване защитата при обработка на лични данни в приложения за електронни услуги към гражданите.

3. Да изготви в пълен обем правила и процедури за защита на личните данни, като за всяка една от подържаните в НАП информационни системи да се разработят правила за обработка на личните данни в тях.

4. Да предвиди в политиките за формиране на профилите за достъп до приложенията (P. By D.), реализиращи електронни услуги за гражданите, достатъчно рестриктивни мерки за достъп до базите данни, като същите да не се достъпват с прекомерни права от привилегированите потребители.

5. Да се предприемат необходимите действия за създаване на одитни записи на отделните събития и дневници /журнали/ за привилегированите потребители. Да се внедрят Система за управление на привилегиите на потребителите (Privileged Access M., PAM) и Система за управление и анализ на събитията, отразени в дневниците (S. information and event management, SIEM).

6. Да се изготви Методика за управление на риска /идентификация на заплахите и оценка на риска), приложима за всяка една информационна система към момента на нейното първоначално въвеждане в експлоатация и последваща периодичност за оценка на риска, съгласно чл. 35 от Регламент (ЕС) 2016/679.

7. Да се извърши анализ на риска на системите и операциите по обработването, включващи изготвени правила и функционални задължения за работа на всяка информационна система.

8. Да се извърши оценка на въздействието при идентифициран „висок риск" за всяка една система и предприетите мерки, съгласно одобрен и публикуван на интернет страницата на КЗЛД списък на по чл. 35, § 4 от Регламент (ЕС) 2016/679.

9. Да се изготвят правила и процедури за оценка на въздействието при защита на данните при първоначално стартиране на нови информационни системи и приложения.

10. Да се стартира процедура по адаптиране на информационните системи към изискванията на Регламент (ЕС) 2016/679, като разработи процедури за управление на риска при въвеждане на нови системи или промяна на вече съществуващи системи (P. By D., P. By Redesign и P. By Default).

11. Да обнови операционните системи от W. 2008R2 към актуални версии от 2013 г. и 2016 г., и на СУБД O. 11.2.0.2 към актуална версия O. 12, за да не се създава потенциална опасност за сигурността на данните след 2020 г., преди изтичане на срока за тяхната поддръжка.

12. Да изгради център за възстановяване работоспособността на системите в реално време (D. R. C.).

13. Да изготви политики за обработване на специални категории данни съгласно чл. 9 от Регламент (ЕС) 2016/679.

14. Да изготви политики за повторно използване на личните данни на субектите.

15. Да изготви политики и вътрешни правила за анонимизиране, архивиране и унищожаване на електронните данни, използвани еднократно.

16. Да изготви политики и процедури за обработка на лични данни на деца, повторното използване на такива данни, проследяващи механизми и Cookies /бисквитки/, определяне срока за съхранение и задържане на данните.

17. Да изготви стратегия и политики за криптиране на данни от архивни или еднократни извършвани справки.
18. Да допълни и/или измени съдържанието на длъжностната характеристика на длъжностното лице по защита на данните, като се впишат ясни правила и задължения за осъществяване на дейността му. Да изготви вътрешни документи, гарантиращи функциите, задълженията и прякото му подчинение на изпълнителния директор, съгласно чл. 38, § 3 от Регламент (ЕС) 2016/679.
19. Да актуализира длъжностните характеристики на служителите на НАП с включени клаузи, касаещи обработването на лични данни.
20. Да изготви вътрешни правила за обучение и тренировка на служителите на НАП за действия в случаи на незаконосъобразно обработване на лични данни.
Определен е и шестмесечен срок за изпълнение на всички разпореждания, считано от датата на получаването им, като за изпълнението им писмено се уведоми КЗЛД и да се предоставят относими доказателства.
Наведените основания за оспорване, предвид изложените в жалбата оплаквания и твърдения се квалифицират от съда по чл.146, т.3 и т.4 АПК-съществени нарушения на адиминстративнопроизводствените правила и противоречие с материалноправните норми-чл.146, т.3 и т.4 АПК. Твърди се, че дадените с оспореното административно решение разпореждания в т.1 до т.20 са много общо формулирани и непълно дефинирани, което създавало неясноти и препятствало тяхното изпълнение. Изразите „ясно разписани правила“, „да се предприемат подходящи технически и организационни мерки“, „пълен обем“, „достатъчно рестриктивни“, „прекомерни“ не били извлечени от конкретни разпоредби или стандарти и не били конкретизирани в самите разпореждания, поради което възпрепятствали възможността на НАП като администратор да изпълни разпорежданията в степен, съответстваща на дадените формулировки. Недостатъчен бил и 6-месечния срок за изпълнение по т.11 и т.12 от оспореното решение, тъй като се изисквало провеждането на процедури по ЗОП. Освен това във връзка с разпореждането по т.12 НАП да изгради център за възстановяване работоспособността на системите в реално време (D. R. C.) с пълна функционалност на информационните системи и услуги на НАП в реално време (резервен център), Агенцията била предприела вече организационни мерки. Независимо от това заложеният от КЗЛД срок бил изключително кратък, тъй като реално процедурите по чл.18, ал.1, т.1 ЗОП можели да отнемат повече от 10 месеца. По отношение разпорежданията на КЗЛД за изготвяне на процедури, правила и политики, следвало да се има предвид, че същите били обосновани от неправилни констатации и изводи на проверяващия екип, а освен това били общи и необвързани с действащ нормативен или друг задължителен за приложение акт. В жалбата са изброени предприетите от НАП технически и организационни мерки за защита при обработването на лични данни, както следва: Система за управлението на бизнес процесите и Системата за управление на сигурността на информацията. Всички процедури в НАП, утвърждавани съобразно чл. 10, ал. 1, т. 5 от Закона за Националната агенция за приходите, били съобразени с международни стандарти за управление на качеството като ISO 9000 и ISO 9001. Същите съдържали секции, които уреждат разпределението, обхвата и предназначението на дейностите, собствениците и клиентите на процеса, детайлно описание на процеса, матрица на разпределение на отговорностите, както и взаимодействието с други процеси. Тъй като НАП обработва голям брой данни, попадащи в обхвата на информация, защитена от закон, като лични

данни, данъчна и осигурителна информация, информация за вътрешно ползване, ограничено ползване и конфиденциална информация, в Агенцията се прилагат действащите политики, правила, процедури, указания и методики за управление на сигурността на информацията в НАП по отношение на всички защитени данни Вътрешните документи, имащи отношение към информационната сигурност и утвърждавани от изпълнителния директор на НАП, са съобразени с изискванията на Закона за електронно управление (ЗЕУ), Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ) и Наредбата за общите изисквания за мрежова и информационна сигурност (отменена на 26.07.2019 г).

В указанието за обозначаване и работа с информация, утвърдено от изпълнителния директор на НАП, е предвидено, че информация, съдържаща лични данни се маркира с „Ограничено ползване“ и са предвидени надлежните организационни и технически мерки за работа с нея. Правилата и процедурите, утвърдени в НАП, свързани със обработването личните данни, са задължителни за изпълнение от всички служители на НАП.

Вътрешните правила не били общи, а регламентират конкретните задължения на служителите на НАП. Те са в съответствие със стандартите и добрите практики за постигане на сигурност на информацията, обработвана в НАП от служителите й.

Поименно определяне на всички привилегировани потребители в НАП със заповед на изпълнителния директор на НАП и достъпване информационните ресурси на НАП, съобразно длъжностната им характеристика и на принципа „необходимо е да се знае“. Бизнес анализатори нямат достъп до бази данни и сървъри, а достъпът им до услуги и системи на Агенцията, е съобразно предоставените стандартни профили за достъп, утвърждавани от изпълнителния директор на НАП. Всички привилегировани права са дефинирани на етап проектиране на информационните системи и услуги на НАП, в изпълнение на процеса проектиране на нова или промяна на съществуваща информационна система/програмен продукт. ; ненарушаване на принципа P. By D. (чл.25 от Регламент (ЕС) 2016/679), поради липса на разработване или внедряване от НАП в периода 25.05.2018 г. - 15.07.2019 г. НАП на нова информационна система или услуга

По отношение на въведените до 25.05.2018 г. електронни услуги, достъпни с квалифициран електронен подпис (КЕП) или с персонален идентификационен код (ПИК) на НАП са разработени при осигурена възможност за проследяване на действията по заявяване и ползване на услугите.

Обекти на системата за информационна сигурност са всички данни в информационните системи на НАП, системната информация, техническите средства, системен и приложен софтуер, електронните и хартиените носители на информация, сгради, сигурни помещения (сървърни, архивни помещения). Всички обекти са подробно инвентаризирани в описи на активи. Защитата на информацията се осъществява на всички етапи на информационния процес - създаване, обработка, съхранение, пренасяне и унищожаване, във всички структури на НАП при извършване на дейностите им.

Всички процедури на НАП са част от внедрената Система за управление на сигурността на информацията и се утвърждават от изпълнителния директор на НАП или овластени от него лица.

Разработване на всички информационни системи на НАП, съобразно вътрешните

процедури на НАП за разработване, тестване и внедряване на информационни системи /ИС/, като в процеса на изпълнение по проектиране на нова или промяна на съществуваща информационна система/програмен продукт се идентифицирали, анализирали и дефинирали всички необходими изисквания с цел осигуряване на сигурност, надеждност, работоспособност и непрекъсваемост на ИС и услуги на НАП. Всички данни в системите и услугите на НАП се разглеждат като информационен актив, който, съгласно одобрената методика за анализ на риска в НАП, се идентифицира, класифицира, оценява, превентира и управлява.

Внедряването на Система за управление и анализ на събития, отразени в дневниците, няма задължителен характер съгласно действащата към момента на инцидента нормативна уредба.

От момента на създаването на информационните системи в НАП съществуват системи за одитиране действията на потребителите. Допълнително са утвърдени правила и процедури, регламентиращи наблюдението на събитията, регистрирани в дневниците за събития от системен и приложен софтуер и мрежови устройства.

На основата на добрите практики в областта, НАП са предприети мерки за планиране и доставка на Система за управление и анализ на събития, отразени в дневниците с цел повишаване на наличните възможности за наблюдение и анализ на събитията в информационните системи на НАП. Системата била включена в тригодишната бюджетна прогноза 2017-2019 г. В началото на 2019 г. било одобрено финансиране за нейната доставка, стартирана била процедура за обществена поръчка и доставката се очаквала в края на годината. В НАП е утвърдена Методика за оценка на риска и процедура за оценка на риска, която обхваща последователността от действия и отговорностите за провеждане на оценка на риска за сигурността на информацията, в съответствие с установената Политика за управление на риска (т. 7 на Политика по информационна сигурност на НАП). В методиката и разработените и утвърдени форми за оценка на риска са идентифицирани заплахите и способите за оценка на риска, които са приложими към всяка една информационна система на всички етапи на нейния жизнен цикъл. В НАП се извършват оценки на риска, при първоначално въвеждане в експлоатация на нови системи, при промяна на системата и периодично, организирано от звеното по мрежова и информационна сигурност.

Оценката на въздействието върху защитата на данните, посочена в случаите по чл. 35, ал. 3 вр. ал. 1 от Регламент (ЕС) 2016/679, не били съотносими към обработването на личните данни в НАП.

Личните данни, които НАП обработва в своите информационни системи, съгласно чл. 72, ал. 1 от Данъчно-осигурителния процесуален кодекс (ДОПК) са включени като част от данъчната и осигурителна информация за задължените лица и субекти и процедурите, свързани със обработването на данъчната и осигурителна информация са същите, с които се обработват и личните данни.

Специални категории лични данни по чл. 9 от Регламент (ЕС) 2016/679 се обработват съгласно чл. 9, пар. 2, б. „б“ от Регламент (ЕС) 2016/679, по смисъла на чл. 87, ал. 2, т. 7 от ДОПК като други обстоятелства, свързани с възникване, промяна и погасяване на задълженията за данъци и задължителни осигурителни вноски. Разпоредбата на чл. 87 от ДОПК определя и съдържанието на данъчно-осигурителната сметка на задълженото лице, което по същество е данъчна и осигурителна информация, която се обработва в НАП за задължените лица. Изпълнителният директор на Националната агенция за приходите утвърждава формата и елементите на данъчно- осигурителната

сметка със заповедта по чл. 81, ал. 2 от ДОПК.
Правилата и процедурите, утвърдени в НАП, свързани с обработването на данните в данъчно-осигурителната сметка, включително и специфични данни, свързани с данъчните и осигурителните задължения, са същите, с които се обработват всички данни в информационните системи като неразделна част от данъчната и осигурителната информация и са задължителни за изпълнение от всички служители на НАП.
Вътрешните правила регламентират конкретните задължения на служителите на НАП. Те са в съответствие със стандартите и добрите практики за постигане на сигурност на информацията, обработвана в НАП от служителите й.
НАП не обработвала специални категории лични данни съгласно чл. 9 от Регламент (ЕС) 2016/679 за цели, извън случаите по чл. 9 пар. 2, б. „б“, за установяването на данъчни и осигурителни задължения и се прилагали политиките и процедурите, свързани с обработването на данъчна и осигурителна информация в НАП, и не било необходимо да се разработват специални правила/процедури, регламентиращи мерките за защита на специалните категории данни, тъй като те се обработвали както данъчна и осигурителна информация и са обект на системата за информационна сигурност.
По отношение на разпореждането за изготвянето на „политики и вътрешни правила за анонимизиране, архивиране и унищожаване на електронните данни“, твърди, че в НАП се прилагат „Вътрешни правила за защита на личните данни на лицата, подаващи сигнали в Националната агенция за приходите“, утвърдени със Заповед №ЗЦУ-174/10.02.2017 г. на изпълнителния директор на НАП, както и Методика за анонимизиране на индивидуални данни, утвърдена със Заповед №ЗЦУ-121 от 30.01.2017 г. на изпълнителния директор на НАП.
Правилата за архивиране и унищожаване на документи, съдържащи лични данни (електронни и на хартиен носител), са регламентирани в Глава четвърта „Организационни и технически мерки за сигурност при обработване на лични данни“ от Инструкция №2 от 08.05.2019 г. за мерките и средствата за защита на лични данни, обработвани в Националната агенция за приходите и реда за движение на преписки и заявяване на регистри, „Указания за унищожаване на информация и информационни носители в НАП“, утвърдени със Заповед №ЗЦУ-1596 от 29.11.2017 г. на изпълнителния директор на НАП.
По отношение съхранението и архивирането на електронни документи и документи на хартиен носител в НАП, се прилагат и разпоредбите на Вътрешни правила за оборот на електронни документи и документи на хартиен носител в НАП, утвърдени със Заповед №ЗЦУ-535 от 11.05.2016 г. на изпълнителния директор на НАП, които са в пълно съответствие с Наредбата за обмена на документи в администрацията и с Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги.
Във всички предоставени длъжностни характеристики било видно и ясно регламентирано мястото на длъжността в структурата на НАП, основната цел на длъжността, областите на дейност, преките задължения, възлагане, планиране и отчитане на работата, отговорностите, свързани с организацията на работата, вземането на решения, взаимодействието, изискванията за заемане на длъжността и необходимите компетентности.

В края на 2018 г. била извършена проверка от ДАЕУ, с обхват изпълнение на изискванията, предвидените в Закона за електронно управление, Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ) и Наредбата за общите изисквания за мрежова и информационна сигурност (отменена на 26.07.2019 г.). Проверката не констатирала нарушения и/или неизпълнение на нормативни изисквания.

В съдебно заседание пред АССГ, процесуалните представители на жалбоподателя-юрк. А. и юрк.М. и юрк. Р. поддържат жалбата и молят за уважаването й. Оспорват заключението на вещото лице по т.1 (л. 576-578) и заявяват искане за присъждане на юрисконсултско възнаграждение. Оспорва приобщаването на третата СТЕ, извършена по друго дело със същия съдия. В депозираните по делото писмени бележки аргументират несъгласието си и с поясненията на вещото лице по първата СТЕ при изслушването му в о.с.з.

Ответникът-КЗЛД, представляван от юрк. П. излага съображения за недопустимост и неоснователност на жалбата, като пледира, че процесното решение на КЗЛД е законосъобразно, а жалбата-неоснователна. Заявява искане за присъждане на юрисконсултско възнаграждение. Поддържа, че от СТЕ се доказали в пълнота фактите, установени при проверката на КЗЛД, а именно че към момента на теча на лични данни липсвали лог-файлове, от които да се установи по какъв начин, от кого точно е извършен достъпа, съответно как е установено изтичането на данните на 6 000 000 български граждани. Към момента на извършване на проверката, както и към момента на изследването от ВЛ, операционната система О. 11.2.0.2 е била в остаряла версия и била актуализирана едва след извършване на проверката от КЗЛД. Всички представени документи от НАП по време на проверката били утвърдени със заповеди преди 2018 г., т.е. НАП не била предприела никакви технически и организационни мерки след приемането на Регламент (ЕС) 2016/679 и дадения със същия двугодишен гратисен период до влизането му в сила през 2018 г. да актуализира вътрешните си правила по отношение на обработката на личите данни, поради което според КЗЛД е възникнал огромният теч на лични данни на български граждани.

Административен съд-София град, след като прецени събраните по делото доказателства и служебно, на основание чл.168, ал.1 от АПК, вр.чл.146 провери изцяло законосъобразността на обжалвания акт, намира следното:

По допустимостта на жалбата.

Жалбата е процесуално допустима.

Преценката за допустимост на жалбата е осъществена с определението от з.з. на 03.10.2019 г. /л. 414/. Налице са положителните, като съответно липсват отрицателните условия, свързани със съществуването и упражняването субективното право на оспорване. Жалбата е подадена от надлежна страна-адресат на акта, за която е налице и пряк и непосредствен интерес от обжалването на засягащите я предписания. Спазен е и преклузивният 14-дневен срок по чл.149, ал.1 АПК - решението е съобщено на жалбоподателя на 23.08.2019 година /л. 151 гръб/, а жалбата до съда е подадена на 04.09.2019 г. /л. 5/.

По основателността на жалбата, съдът излага следното от фактическа и правна страна:

1.Безспорни между страните по делото са следните факти:

1.1 Жалбоподателя НАП е специализиран държавен орган към министъра на финансите за установяване, обезпечаване и събиране на публични вземания и определени със закон частни държавни вземания (чл. 2, ал. 1 от ЗНАП) и администратор на лични данни по смисъла на чл. 4, т. 7 от Общия регламент относно защитата на личните данни. В това качество жалбоподателя обработва личните данни.

1.2 В изпълнение на задълженията си за законосъобразно обработване на личните данни жалбоподателят е приел следните актове и е извършил следните действия:

1. Указания за обозначаване и работа с информацията, утвърдени със Заповед № ЗЦУ-1595 от 29.11.2017 г. на изпълнителния директор на НАП; 2. Политика по информационна сигурност на НАП; 3. Инструкция № 2 от 08.05.2019 г. за мерките и средствата за защита на лични данни, обработвани в НАП и реда за движение на преписки и заявяване на регистри; 4. Процедура № ПФИС7, Версия В Оценка на риска за информационната сигурност, вкл. Методика за оценка на риска, утвърдена от изпълнителния директор на НАП на 17.06.2016 г.; 5. Заповед № ЗЦУ-733 от 17.06.2016 г., с която са утвърдени вътрешни правила за мрежова и информационна сигурност.; 6. Заповед № ЗЦУ-1436 от 15.10.2018 г. на изпълнителния директор на НАП, с която са утвърдени Указания за разработване, попълване и/или зареждане с данни на образци на документи и приложения, утвърдени на основание чл. 10, ал. 1, т. 5 и т. 7 от ЗНАП, използвани в изпълнение на действащите процедури и инструкции; 7. Заповед № ЗЦУ-482 от 01.04.2019 г. относно определяне на служители на НАП, с администраторски достъп до информационните активи и услуги на НАП; 8. Процедура № ИС17, Версия В, Администриране на информационна система в НАП, утвърдена със Заповед № ЗЦУ-1236 от 21.08.2019 г. на изпълнителния директор на НАП; 9. Заповед № ЗЦУ-586 от 30.04.2014 г. на изпълнителя директор на НАП относно внедряване на Система за управление на сигурността на информацията (С.) в НАП.; 10. Заповед № ЗЦУ-93 от 23.01.2013 г. на изпълнителния директор на НАП относно вида, съдържанието, реда за създаване, поддържане и достъп до регистъра на НАП и базите данни за задължените лица, формата и елементите на данъчно-осигурителната сметка и сроковете за съхранение на архивната информация; 11. Методика за анонимизиране на индивидуални данни, утвърдена със Заповед № ЗЦУ-121 от 30.01.2017 г. на изпълнителния директор на НАП; 12. Вътрешни правила за защита на личните данни на лицата, подаващи сигнали в НАП, утвърдена със Заповед № ЗЦУ-174/10.02.2017 г. на изпълнителя директор на НАП; 13. Указания за унищожаване на информация и информационни носители в НАП, утвърдени със Заповед № ЗЦУ – 1596 от 29.11.2017 г. на изпълнителния директор на НАП; 14. Вътрешни правила за оборот на електронни документи и документи на хартиен носител в НАП, утвърдени със Заповед № ЗЦУ-535/11.05.2016 г. на изпълнителния директор на НАП.

1.3. Административното производство пред КЗЛД е започнало по изпратено от

НАП Уведомление вх. № ППН-02-399/17.07.2019 г. по чл. 33 от Регламент (ЕС) 2016/679, в което е посочено, че на 15.07.2019 г. е установен неоторизиран достъп до обработваните от НАП бази данни с лични данни (име, ЕГН), като съдържаща се в тях информация е публикувана в интернет пространството /л. 172-176 по делото/.
1.4. На 18.07.2019 г. е представена пред КЗЛД докладна записка за извършен анализ на постъпилото Уведомление вх. № ППН-02-399#1/18.07.2019г. (л.180-184/ На проведено на 19.07.2019 г. заседание КЗЛД се самосезира във връзка с публикации в медиите за извършен пробив в сигурността на данните в НАП, като към образуваното производство е приобщено и полученото уведомление от страна на НАП. Прието е решение за извършване на проверка с Протокол № 31/19.07.2019г. в раздел „I – Доклад на Дирекция „Правни производства и надзор“ “ (л. 179).
1.5. Със заповед № РД-15-249 от 19.07.2019 г. на председателя на КЗЛД е определен проверяващ екип (л. 170), изпратено е уведомление до НАП (л. 185-186/ и проверката е открита на 22.07.2019 г. в административната сграда на ЦУ на НАП в [населено място], като е изпратен въпросник за проверката (л. 187-191) (а впоследствие и втори – л. 192-193), касаещ структурата, основните направления на дейност, предприетите технически и организационни мерки за защита на данните относно физическата, персоналната, документалната защита, защитата на автоматизираните информационни системи и/или мрежи и криптографска защита. НАП изпълнява разпорежданията на КЗЛД за представяне на отговори /л. 194-223/ и в отговор на искане с вх. № ППН-02-399#117/13.08.2019 г. (л. 256-287 и л. 291-354/ от 14.08.2019 г. свързан с Въпросник № 2 /. С Констативен протокол от 02.08.2019 г. и 08.08.2019 г. се установява, че са проведени работни срещи с определени от НАП длъжностни лица за оказване на съдействие на проверяващия екип (л. 224-227 и л. 229/.
1.6. С писмо изх. № ППН-02-399#92 от 07.08.2019 г. от специализираната прокуратура е поискано предоставяне имената на всички вероятно изтекли папки с данни, като те са предоставени на 08.08.2019 г. (л. 252-255) . На 13.08.2019 г. с писмо с изх. № ППН-02-399#116 от НАП е изискан доклад за констатациите и препоръките на ДАНС, който е бил представен (л. 230-231). На същата дата бил съставен приемо-предавателен протокол за предаване на следните документи: 1) Писмо рег. № ДАЕУ – 12345/12.12.2018 г. 2) Писмо рег. № ЕП-2339#1/19.12.2018 г.; 3) Заповед ЗЦУ – 744/22.05.2019 г.; 4) Заповед ЗЦУ – 747/25.05.2018 г.; 5) Длъжностна характеристика старши експерт главен експерт, отдел ВСЗИ, дирекция „Сигурност“; 6) Длъжностна характеристика главен експерт, отдел Р., дирекция ИСМБП; 7) Длъжностна характеристика главен експерт, отдел АБДС, дирекция ИСМБП; 8) Длъжностна характеристика главен експерт, сектор УИ, отдел УЕИ, дирекция ИСМБП (л. 232-251) .
На 14.08.2019 г. бил съставен приемо-предавателен протокол по искането за предоставяне на информация за списък и брой на починали лица, Заповед ЗЦУ -745/25.05.2018 г. и Заповед ЗЦУ-744 от 22.05.2019 г., както и утвърден регистър на категориите дейности по обработване (л. 270 и л. 288-291 и л. 355-357) .
На същата дата- 14.08.2019 г. е бил съставен друг приемо-предавателен

протокол за представяне на пет заверени копия на документи, а именно: 1) Инструкция № 2/08.05.2019 г. за мерките и средствата за защита на лични данни, обработвани в НАП и ред за движение на преписки и заявяване на регистри; 2) Политика по защита на личните данни в НАП утвърдена със Заповед № ЗЦУ – 746/25.05.2018 г.; 3) Процедура ПРЗ „Оказване на методическа помощ за обработване и защита на информацията“, версия А, утвърдена със Заповед № ЗЦУ – 235/06.03.2015 г.; 4) Разпечатка на рубриката „Юридическа информация“ публикувана на официалната интернет страница на НАП относно ползването на информационни ресурси на интернет страницата и на мобилното приложение; 5) Съобщение до гражданите публикувано на официалната интернет страница на НАП /л. 358-382/.
На 15.08.2019 г. е бил съставен друг приемо-предавателен протокол, представен на магнитен носител, който съдържа: 1) G. matrix за потребител “VATREFUND”, актуална към 15.07.2019 г.; 2) Допълнителна информация към представени списъци на всички активни физически лица, разделени в отделни файлове по критерий вид на идентификатора; 3) Преписка във връзка с получено заявление по Закона за достъп до обществената информация с вх. М-26-Н-23/09/06.2017 г.; 4) Екранни разпечатки от екраните на деловодна система „А.“, от които са видни данни за движението по преписката – номера и дати на служебни бележки и други документи, както и отговорни дирекции и служители; 5) Списък на структурирани и окрупнени информационни активи с оценка на риска за всеки актив /л. 383-413/.
На 20.08.2019 г. бил съставен Констативен акт (КА) с вх. № ППН-02-462 /л. 152-168/, който служи за основание за издаването на Индивидуалния административен акт (ИАА) на КЗЛД – Решение № ППН-02-399 от 22.08.2019 г. (л. 147-151).
1.7. *НАП узнава за нерегламентирания достъп до нейните информационни масиви от информация, публикувана на 15.07.2019 г. в интернет пространството*.
Броят на физическите лица, до чиито данни е осъществен неоторизиран достъп и същите са разпространение /актуален към 20.07.2019 г./ е, както следва:
-общ брой на всички физическите лица, което включва български и чужди граждани, в това число с прекратена регистрация - 6 074 140 бр.;
- общ брой на всички активни физически лица, което включва български и чужди граждани-4 104 786 бр.;
- общ брой на активните български граждани /с ЕГН/ - 4 057 328 бр.;
-общ брой на активните чужди граждани с личен номер на чужденец /ЛНЧ/ - 24 507 бр.;
- общ брой на физическите лица /български и чужди граждани/ под 18-годишна възраст от общия брой активни български и чужди граждани - 8 402 бр.;
- общ брой на неактивни /с прекратена регистрация/ български граждани с ЕГН/ - 1 959 598 бр.;
- общ брой на неактивни /с прекратена регистрация/ чужди граждани с личен номер на чужденец /ЛНЧ/ - 9 425 бр.;
- общ брой на неактивни /с прекратена регистрация/ чужди граждани със

служебен номер на НАП - 351 бр.;
- 154 броя идентификатори на физически лица /български и чужди граждани/ се срещат като повече от един тип идентификатор /ЕГН, ЛНЧ, служебен номер на НАП/;
- общ брой физически лица, за които, видно от публикуваната информация на интернет страницата на НАП, е достъпена следната информация: имена, ЕГН, адрес, номер, валидност и издател на валидна лична карта - 189 бр.;
- общ размер на информацията, до която е осъществен неоторизиран достъп и е разпространена в интернет пространството - minfm_leak.zip - 1,71 GB или 10,7 GB в разархивиран вид;
- общ брой на папките, съдържащи се в minfm_leak.zip - 57 бр.; е общ брой на файловете /*.csv/, съдържащи се в minfm_leak.zip - 1044 бр.;
- общата големина на базата, която се намира на сървъра в НАП, до който е осъществен неоторизиран достъп - 1 733 GB;
-частта от информация, която се намира на сървъра в НАП, от разпространените 57 папки в minfin_leak.zip, в съвкупност с прикачените декларации и файлове (LOB файловете), до който е осъществен неоторизиран достъп - 1450 GB;
- частта от информация, която се намира на сървъра в НАП, от разпространените 57 папки в minfm_leak.zip, без прикачените декларации и файлове (LOB файловете), до който е осъществен неоторизиран достъп - 427 GB.
- сървърът до който е осъществен нерегламентираният достъп работи с остаряла версия на операционната система W. 2008R2 и по-стара версия на СУБД O. 11.2.0.2. Системното и базово програмно осигуряване не е обновявано, защото приложните системи няма да работят с по-новите им версии и трябва да се модифицират.
1.8. С Докладна записка за извършена вътрешна проверка от Инспектората на НАП, представена на КЗЛД на 13.08.2019 г. с писмо № ППН-02-399#117/2019 г. , при която проверяващите са установили, че неправомерно разпространените файлове съдържат следните категории лични данни:
- имена, ЕГН и адреси на български граждани;
- телефони, електронни адреси и друга информация за контакт; о данни от годишни данъчни декларации на физически лица;
- данни от справките за изплатени доходи на физически лица;
- данни от осигурителни декларации;
- данни за здравноосигурителни вноски.
Следва да бъде посочено, че що се отнася до информацията за медицински статус или информация за лечение на гражданите, тя бива спорна по делото ;
- данни за издадените актове за административни нарушения;
- данни за извършените плащания на данъци и осигурителни задължения през „Български пощи” АД;
- данни за поискан и възстановен ДДС, платен в чужбина, т.нар. V. Refund:
-данни за задължено лице /ЗЛ/, подало заявление за възстановяване на ДДС- име, имейл, адрес;
-данни за извършени покупки/внос на български ЗЛ - данъчна основа и ДДС, име на доставчика, идентификатор на доставчика, адрес;

-данни за покупки на български ЗЛ за 2009-2010 г. - данъчна основа и ДДС, име на доставчика, идентификатор на доставчика, адрес;
-данни за издателя и получателя на решението за възстановяване - RO потребителски имена и имейли на заявител и агент, ДДС номер на заявителя;
-три имена на служители на НАП - потребители на системата с съответните RO, електронен адрес, длъжност, пароли;
- данни, свързани с информационни системи М. / VoES:
-BIC, IB AN, име и адрес на банките, посочени за превеждане на суми между ДЧ на ЕС;
-pdf файлове на актове за възстановяване на надвнесени суми;
-регистрационни данни на лица на рег. по М. - имена, ДДС номера, адреси, имейли и интернет адреси, телефони, лица за контакти, данни за постоянни обекти, предходни регистрации;
-данни за декларациите подадени от български/чуждестранни ЗЛ - ДЧК, данъчна основа, ставка ДДС;
-данни за плащанията по декларации;
-данни от международния обмен на данъчна информация за български местни лица;
-служебни данни, получени от други институции в НАП, като Агенция Митници /АМ/, Агенция по заетостта /АЗ/, Агенция за социално подпомагане /АСП/, Националната здравноосигурителна каса /НЗОК/, и др.
1.9. Информацията, която е неправомерно достъпена и впоследствие оповестена публично в интернет пространството включва, както следва:
-информация, обменяна, обработвана и съхранявана в информационни системи, разработени съгласно изисквания на Европейската комисия и други външни институции - О.:
- данни от система за автоматизиран обмен на информация /AEOI/ в НАП /DAC 1/ - за доходи от трудови правоотношения; възнаграждения по договори за управление и контрол; застрахователни обезщетения; пенсии; собственост и/или доходи от продажба или замяна на недвижимо имущество; доходи от наем;
- данни от система за автоматизиран обмен на информация за финансовите сметки със страните-членки на ЕС /DAC 2/ и юрисдикции О. /С./;
- данни от специална схема за облагане с ДДС – съкратено обслужване на едно гише /информационни системи М. и VOES /;
- данни от програмен продукт EUROFISC - борба с данъчните измами на европейско ниво.
-информация, обменяна, обработвана и съхранявана в информационни системи, разработени съгласно изисквания на националното законодателство:
-подаване на данни от организатори на хазартни игри от разстояние съгласно изискванията на Наредба № 1/2013 г. към Закона за хазарта - съдържа лични данни за идентификатори, имена на лица, данни от документи за самоличност, направени залози и печалби;
-ИС Контрол на горивата: извадка от данни от комуникационния модул с лица, регистрирани по Закона за митниците на АМ; данни от електронни акцизни данъчни документи (ЕАДД) и митнически декларации (незначещи) и регистрационни данни за Електронната система с фискална памет (ЕСФП) от

НАП;
- информация за лица от АСП - ЕГН, име на файл от АСГ1, имена на лицето, код за грешка, код за наличие на ЕТ, сума на доходи от декларация по чл. 50 от ЗДДФЛ;
- данни от осигурителни декларации за лица, подадени от АСП до 2017 г.; о информация за лица от АЗ - ЕГН, имена; от НАП - код за грешка, имена, кодировка за наличие/липса на декларация обр.1, дата на създаване на записа, дата на обработка, Ш на файла от АЗ, флаг за наличие на декларация по чл. 50 от ЗДДФЛ;
- регистър Административнонаказателни преписки - данни от Протоколи, АУАН и НП на лица и данни за лицата;
- данни от подадени декларации по чл. 50 от ЗДДФЛ, чл. 92 от ЗКПО и Справката по чл. 73, патентни декларации;
- данни за платени суми за данъчни и осигурителни задължения от лица през „Български пощи" АД до 2018 г.;
- електронен регистър за обезпечаване на дейността по административното сътрудничество с ДЧ на ЕС при събиране на публични вземания - Информационна система „Взаимна помощ при събиране";
- информация от НЗОК за лица с декларация по § 19и от Преходните и заключителни разпоредби на Закона за здравното осигуряване;
- списък с 1 064 млн. идентификатора и данни за заплата, данъци осигуровки;
- регистрационни данни за физически и юридически лица;
- лични данни за служители на НАП към 2009 г.; лични данни за физически лица от Главна Дирекция „Гражданска Регистрация и Административно Обслужване" /ГДГРАО/; лични данни за съдии, следователи и прокурори; лични данни за висши държавни служители; данни с линкове и адреси на приложения в НАП.;
- данни от система „Въпроси и отговори";
-данни от програмен продукт „Заеми" - предоставени/получени заеми от физически/юридически лица;
- данни от програмен продукт „Регистър за консултации";
- данни за продадени бандероли и начислен акциз до 2006 г.
1.10. В хода на проверката НАП потвърждават, че информацията с лични данни, до която е осъществен нерегламентиран достъп и която е публикувана в интернет пространството, е част от нейните информационни масиви. Посочват, че достъпът е осъществен поради техническа уязвимост на информационните системи и пропуски в конфигурациите на мрежово ниво, изброени в доклада на Инспектората на НАП рег. № 93-00-1383 от 22.03.2019 г.(л.425-431) .
2. Изводите на КЗЛД, с които са аргументирани дадените предписания са следните:
2.1 Организационна структура – има изградена структура за защита на личните данни. Определени са видовете потребители в информационните системи на НАП (собственици на данни, разработчици, системни администратори, бизнес анализатори, администратори на бази данни, администратори на приложенията и органи по сигурността на данните), но в хода на проверката не са предоставени правила за отделните потребители,

функционалните им задължения и процедурите за тяхната дейност. Не са достатъчно ясно разписани принципите на взаимодействие на отделните потребители. Липсват процедури за взаимодействие на отделните потребители в системата за защита на личните данни.
2.2. Продължителното самостоятелно разработване на приложения за електронни услуги към гражданите е дебалансирало системата за защита на данните, като тежестта е изместена към функционалността на услугите в полза на гражданите за сметка на необходимата защита при обработване на данните на данъчнозадължените лица.
2.3. Основните отговорности за информационната сигурност са съсредоточени в ИТ дирекцията. Липсват разписани правила и процедури за защита на личните данни, а са налице само такива, които касаят информационната сигурност (киберсигурността). Вътрешните правила са общи. За всяка една от подържаните в НАП информационни системи, следва да се разработят правила за обработка на личните данни в тях. Необходимо е да се има предвид, че киберсигурността е само част от мерките за защита на личните данни и е задължително разработването на правила/процедури, регламентиращи мерките за защита на различните категории лични данни, като цяло и съобразно техният вид и чувствителност (съобразно оценката на риска).
2.4. Към датата на неоторизирания достъп и разпространението на личните данни на 15.07.2019 г., в политиките за формиране на профилите за достъп до приложенията (P. By D.), реализиращи електронни услуги за гражданите, не са предвидени достатъчно рестриктивни мерки за достъп до базите данни, като същите са достъпвани с прекомерни права (привилегировани потребители). Определените привилегировани потребители имат достъп до целия информационен ресурс с изключение на системните ресурси, осигуряващи работоспособността на базите данни. С правата на привилегировани потребители са всички разработчици на приложения, бизнес анализатори, както и всяко едно приложение (услуга). Към момента на проверката проверяващият екип констатира, че достъпът е ограничен само до собствените схеми, като ограничението не нарушава функционалността на съответното приложение и предлаганите чрез него услуги. Ограничаването на правата е следвало да бъде направено към момента на проектирането.
2.5. Нарушен е принципът на отчетност - липсват одитни записи на отделните събития и дневници (журнали) за привилегированите потребители. Няма внедрена Система за управление на привилегиите на потребителите (Privileged Access M., PAM), с оглед контрол, управление и наблюдение на привилегирован достъп до критични активи.
Не е внедрена и Система за управление и анализ на събитията, отразени в дневниците (S. information and event management, SIEM), с оглед одитиране на дейностите на потребителите в системата и осигуряване на анализ в реално време на сигналите за сигурност, генерирани от мрежовия хардуер и приложения.
2.6. Липсва методика за управление на риска (идентификация на заплахите и оценка на риска), приложима за всяка една информационна система към момента на нейното първоначално въвеждане в експлоатация и последваща

периодичност за оценка на риска, съгласно чл. 35 от Регламент (ЕС) 2016/679.
2.7. Не са представени доказателства за извършен анализ на риска на системите и операциите по обработването, включващи изготвени правила и функционални задължения за работа на всяка информационна система.
2.8. Не са представени доказателства за извършена оценка на въздействието при идентифициран „висок риск" за всяка една система и предприетите мерки (съгласно одобрен и публикуван на интернет страницата на КЗЛД списък на по чл. 35, параграф 4 от Регламент (ЕС) 2016/679).
2.9. Липсват документирани правила и процедури за оценка на въздействието при защита на данните при първоначално стартиране на нови информационни системи и приложения.
2.10. Няма данни за стартирана процедура по адаптиране на информационните системи към изискванията на Регламент (ЕС) 2016/679. Липсват процедури за управление на риска при въвеждане на нови системи или промяна на вече съществуващи системи (P. By D., P. By Redesign и P. By Default).
2.11. Не са предприети действия за обновяване на операционните системи от W. 2008R2 към актуални версии от 2013 г. и 2016 г., и на СУБД O. 11.2.0.2 към актуална версия O. 12, което създава потенциална опасност за сигурността на данните след 2020 г., когато изтича срокът за тяхната поддръжка.
2.12. Няма изграден център за възстановяване работоспособността на системите в реално време (D. R. C.).
2.13. Липсват политики за обработване на специални категории данни съгласно чл. 9 от Регламент (ЕС) 2016/679.
2.14. Липсват политики за повторно използване на личните данни на субектите.
2.15. Липсват политики и вътрешни правила за анонимизиране, архивиране и унищожаване на електронните данните, използвани еднократно (различни видове
справки и заявки).
2.16. Липсват политики и процедури за обработка на лични данни на деца, повторното използване на такива данни, последващи механизми и Cookies (бисквитки), определяне срока за съхранение и задържане на данните.
2.17. Липсват приети стратегия и политики за криптиране на данни от архивни или еднократни извършвани справки.
2.18. Нарушен е принципът на независимост на длъжностното лице по защита на данните (намира се в йерархична подчиненост на директора на Дирекция „Сигурност“). В длъжностната му характеристика не са вписани ясни правила и задължения за осъществяване на дейности като длъжностно лице по защита на данните. Не са изготвени вътрешни документи, гарантиращи функциите, задълженията и прякото му подчинение на изпълнителния директор.
2.19. Служителите на НАП подписват декларация за неразпространяване на информация, но в длъжностните им характеристики няма включени задължения за обработване на лични данни на физически лица при изпълнение на конкретните им служебни задължения. Не са актуализирани длъжностните характеристики с включени клаузи, касаещи обработването на лични данни.

2.20. Липсват вътрешни правила за обучение и тренировка на служителите на НАП за действия в случаи на незаконосъобразно обработване на лични данни.
3. По делото са изготвени 2 СТЕ (л.566-574 и л.647-658) и заключението по още една (667-672) е приобщено към доказателствата по делото. Заключенията са изготвени от лица със специални познания в областта на информационните технологии и киберсигурността, за да се отговори на въпросите дали взетите мерки от НАП са подходящи и достатъчни за защита на личните данни на гражданите, както и да се установи имало ли е действия, които е трябвало да бъдат извършени, а не са.
В изпълнение на указания на съда, дадени с определение от 30.05.2022 г. (л. 659) жалбоподателят е представил Резюме на препоръките на Глобалния форум съдържащо и конкретен списък с предприети защитни мерки и подобрения на информационната система на НАП в изпълнение на дадените му препоръки. Препоръките представят статуса на НАП към 15.11.2021 г.
В изпълнение на указания на съда, дадени с разпореждане от 07.03.2022 г. жалбоподателят е представил заверен препис от доклада на Временната анкетна комисия, приет от Народното събрание на 20.02.2020 г. (л. 609-646). Точка втора на „Констатации и препоръка“ гласи, че ръководството на НАП следва да се съобрази с констатациите от доклада на КЗЛД при извършената проверка от месец август тази година.
Жалбата е частично основателна, поради следните съображения:
Оспореното решение е издадено от компетентен орган- КЗЛД. Съгласно чл. 6, ал. 1 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.
Тази своя функция Комисията осъществява упражнявайки предоставени от закона правомощия, посочени в чл. 10, ал. 1 ЗЗЛД.
Обжалваното решение е прието е при необходимия кворум и с необходимото мнозинство - арг. чл. 9, ал. 3 от ЗЗЛД и чл. 8, ал. 6 и ал. 7 от Правилника. Съгласно чл. 7, ал. 1 от ЗЗЛД комисията е колегиален орган и се състои от председател и 4 членове, а решенията се вземат с мнозинство от общия брой на членовете (чл. 9, ал. 3). Същото следва да бъде подписано от всички членове, участвали в гласуването. В случая за оспореното решение са гласували четирима със "за" и нито един против, поради което безспорно е формирано мнозинство и решението е валидно взето. В тази връзка не е осъществено основанието по чл. 146, т. 1 АПК.
Спазена е установената от закона форма - актът е в писмена форма, посочени са фактическите и правни основания за издаването му. Същият съдържа изискуемите от разпоредбата на чл. 59, ал. 2 АПК реквизити, доколкото приложимият специален закон - ЗЗЛД не съдържа специални изисквания към формата и съдържанието на акта. Оспореният акт съдържа ясна разпоредителна част, посочени са релевантните факти и обстоятелства и приложимите според административния орган правни норми, проявлението на които обосновава разпоредените от него правни последици.
В производството не са допуснати съществени нарушения на административно-производствените правила, свързани с правото на участие

на жалбоподателя и възможността да прави възражения и да представя доказателства. Производството е започнало по изпратено от НАП Уведомление вх. № ППН-02-399/17.07.2019 г. по чл. 33 от Регламент (ЕС) 2016/679 и на 19.07.2019 г. КЗЛД се е самосезирала и след обсъждане на КА акт рег. № ППН-02-462/20.08.2019 г. е взето процесното решение.

По отношение изискването за мотивираност на акта съдът напомня, че съгласно Тълкувателно решение № 16 от 31.III.1975 г., ОСГК на Върховния съд мотивите към административния акт могат да бъдат изложени и отделно от самия акт най-късно до изпращането на жалбата срещу акта, в препроводителното писмо или в друг документ към изпратената преписка. В този смисъл КА, рег. № ППН-02-462/20.08.2019 г. следва да се цени като мотиви към процесното решение на КЗЛД. По отношение на някои от разпорежданията обаче липсват необходимите мотиви, което ще бъде изложено при конкретното им обсъждане по долу, заедно с прценката за правилното приложение на материалния закон.

Предварително и преди всичко обаче следва да се посочи, че разпоредбата на чл. 59, ал. 1 от ЗЗЛД задължава ответника не само да прилага подходящи технически и организационни мерки, за да гарантира обработването на данните в съответствие с този закон, но и да е в състояние да докаже това. В този смисъл е и разпоредбата на чл. 24, § 1 от Общия регламент. Изискването за доказване на законосъобразното обработване на данните, разписано като законово задължение на администратора обръща доказателствената тежест, като я възлага върху администратора. Казано по друг начин разпоредбите на чл. 59, ал. 1 от ЗЗЛД и чл. 24 от Общия регламент създават оборима презумпция за незаконосъобразното обработване на личните данни, ако администраторът не докаже, че обработването им в съответствие със закона.

В тази връзка съдът сочи още, че съгласно чл. 45, ал. 1, т. 6 от ЗЗЛД данните се обработват по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. Разпоредбата възпроизвежда съображение 83 и чл. 5, пар. 1, б. „е“ от Регламент 2016/679. В чл. 66, ал. 2 от ЗЗЛД законодателят е посочил изрично, но не изчерпателно, мерките които администраторът е длъжен да вземе за защита не обработваните данни. Разпоредбата на чл. 4, § 12 от Общия регламент изрично определя като "нарушение на сигурността на лични данни" това нарушение, 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.

По делото са представени доказателства за мерките, които жалбоподателят е взел, но въз основа на представените административни актове не може да се установи дали мерките са приложени, от една страна, нито дали са достатъчни и подходящи, от друга. Представянето на писмени доказателства не е достатъчно да обоснове такъв извод. Тези факти могат да бъдат

установени само чрез съдебно-техническа експертиза, извършена от лица със специални знания в областта на информационните технологии и киберсигурността, след като им се предостави достъп до информационните системи на жалбоподателя. Поради тази причина изводите на съда ще бъдат обосновани от заключенията по трите СТЕ, приети по делото.
Що се касае до възражението на жалбоподателя за отвод на съдията-докладчик, свързан с приетата третата СТЕ (л. 677) следва да бъде повторена аргументацията на съда, изложена в протокола от 19.09.2022 г. (л. 678). Изпълнението на задължението на съда да събере всички възможни доказателства за обективното пълно и всестранно изясняване на спора от фактическа страна, още повече на спор с такава голяма обществена значимост, като процесния, по никакъв начин не сочи предубеденост на съдията. Точно обратното, процесуалните действия на съдията са насочени изцяло към установяване на обективната истина по спора. Попълването на делото с всички възможни доказателства по никакъв начин не индицира кои доказателства ще бъдат ценени и до каква степен кредитирани, нито пък сочи на изопачаване, игнориране или друго недопустимо процесуално действие, свързано със събирането и преценката на доказателствата по делото. Ноторно известен факт е, че в административните съдилища са били образувани стотици дела във връзка с претендирани обезщетения по ЗОДОВ от граждани, чиито лични данни са попадали сред изтеклите през 2019 г. Доведена до край логиката на жалбоподателя би означавала да няма съдия, който е в състояние да разгледа спора, тъй като почти всички административни съдии са разглеждали спорове във връзка с теча на лични данни през 2019 г. На последно място няма пречка да се приобщи заключение, извършено по друго дело към доказателствените материали по настоящото дело, ако е спазен процесуалният способ, установен за това-чрез устно изслушване на вещото лице в открито съдебно заседание под страх от наказателна отговорност (чл.200, ал.1 и ал.2 ГПК, вр.чл.144 АПК) и приемане на депозираното писмено заключение, което в случая съдът направи.
Конкретно по отношение на оспорените двадесет разпореждания, съдът излага следното:

1. Разпореждане № 3 и Разпореждане № 13 се разглеждат заедно, тъй като се отнасят до обработване на специална категория лични данни. Според заключението по първата СТЕ (л. 566-574), Указанията за обозначаване и работа с информация версия 3.1 от 2018 г. (л. 15-18) съдържат кратки указания за работата, видовете информация и начина на разпространение на тези видове между служители на НАП и извън агенцията. Документът не съдържа конкретни правила за обработка на лични данни. Относно „Политика по информационна сигурност на НАП“, версия 3, от май 2016 година, вещото лице сочи, че липсва конкретна информация за обработка на лични данни. Що се касае до Заповед № ЗЦУ 746 / 25.05.2018 г., която се утвърждава политика за защита на личните данни (369-371), тя представлява документ от 4 страници, написан на популярен език и насочен към лицата ,на които НАП обработва личните данни. Документът съдържа основни определения и тълкувания на понятията свързани със защитата на лични данни. Коментирана е и Заповед ЗЦУ – 585/24.03.2021 г. с утвърдени роли за достъп

до информационните системи на НАП, където се обработвали и визуализирали различен по обхват данни и се създават коректни правила за защита на различните категории лични данни. Съдът приема, че тази заповед, тъй като е след датата на издаване на оспореноторешение не следва да се коментира при преценката за законосъобразност. Други документи само са споменати, без да бъде представена оценка. Становището на вещото лице по първата СТЕ е, че е установено наличието на няколко документа съдържащи кратки указания, основни определения и тълкувания на понятията свързани със защита на лични данни, които не съдържат конкретни правила за обработка на личните данни в отделните поддържани в НАП информационни системи. Посочва се още, че според служителите в НАП не се обработват специални категории лични данни съгласно чл. 9 от Регламент 2016/679, като религия, пол, интереси и др, както и че в изследваните от него информационни системи на НАП не е установил лични данни съдържащи информация разкриваща расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични данни или биометрични данни. В о.с.з. на 04.01.2022 г. вещото лице К. сочи, че в различни периоди НАП създава много документи с различни инструкции и правила, касаещи личните данни, но те не са обединени и структурира в единна политика или единен йерархичен документ. Това създава проблеми при ползването. Посочва, че е запознат с Инструкция № 2, която касае различни дейности в НАП, но тя не съдържа детайлни указания за всички дейности, които са необходими във връзка със сигурността на данните.

Със заключението по втората СТЕ /л. 647-658/ се установява, че към 15.07.2019 г. НАП разполага с няколко документа, в които са заложени основни правила и общи кратки указания и тълкования свързани със защита на лични данни. В тези документи не са регламентирани конкретни правила за събиране, обработване и съхранение на лични данни в и чрез притежаваните и използваните информационни системи от НАП. Не са открити процеси и необходимост от събиране, обработване и съхранение на чувствителни лични данни /етнически произход, политически възгледи, сексуална ориентация, религиозни възгледи и др./, което не задължавало НАП да изготвя специални правила за това. Предприетият от НАП модел за осигуряване на защита на лични данни чрез общи, а не конкретни правила и изисквания е базиран на внедрена Система за Управление на Информационната Сигурност /С./, базирана на международно признатия стандарт за сигурност на информацията БДС ISO/IEC 27001/2014. Правилата и изкисванията в този стандарт са по-разширени от изискванията, заложени в Регламент 2016/679 и следва да се приемат за достатъчни при осигуряване на защитата на личните данни. В о.с.з на 30.05.2022 г. при изслушването му вещото лице В. пояснява, че информацията, която сочи ответника на стр. 5 от писмените бележки депозирани на 14.02.2022 г. се съдържа в информационните системи. Лично я е видял, това е същата информация, която се съдържа във формулярите на данъчните декларации. Сочи се увреждането и трайно намалената работоспособност, без да се конкретизира конкретното заболяване, което е довело до това. Поради тази причина той е приел, че няма необходимост и

НАП не е длъжна да изготвя специални права в отговора на въпрос 1 от заключението. Уточнява, че И. стандарта е международен стандарт за информационна сигурност. В него се дават най-общите минимални правила, които следва да спазва всяка една организация, като след това развитието на Регламент 2016/679 в частта за осигуряване на информационната сигурност, също стъпва върху този признат международен стандарт.

1.1 С оглед на горните констатации следва да се отбележи, че съдът изцяло кредитира изводите и на двете СТЕ в частта, за това, че приетите документи от НАП към датата на установяване на изтичането на информация съдържат само основни правила и общи кратки указания свързани със защитата на личните данни, като не се регламентирани конкретни правила за събиране, обработване и съхранение на лични данни в и чрез притежаваните и използваните информационни системи от НАП.

1.2 Относно констатацията, че не се съдържат чувствителни лични данни и НАП не е бил длъжна да изготви специални основания за това, следва да се отбележи, че в заключението по първата СТЕ не е даден пример за чувствителна информация, а по втората СТЕ вещото лице сочи, че не е констатирало събирането на информация за здравословното състояние на лицата. В същото време, съгласно изложеното в о.с.з при изслушването на вещото лице В., се потвърждава, че НАП събира данни за увреждането и процент трайно намалена работоспособност на лица. Тези противоречиви констатации не могат да намерят своето логично обяснение. Преди да бъде разгледан въпросът по същество е важно да бъде припомнено значението на това понятието в светлината на правото на Европейския съюз. Съгласно съображение 35 от Регламент 2016/679 личните данни за здравословното състояние следва да обхващат всички данни, свързани със здравословното състояние на субекта на данните, които разкриват информация за физическото или психическото здравословно състояние на субекта на данните в миналото, настоящето или бъдещето. Т*ова включва информация относно физическото лице, събрана в хода на регистрацията за здравни услуги или тяхното предоставяне, както е посочено в Директива 2011/24/ЕС на Европейския парламент и на Съвета, на същото физическо лице; номер, символ или характеристика, определени за дадено физическо лице с цел уникалното му идентифициране за здравни цели*; информация, получена в резултат от изследването или прегледа на част от тялото или на телесно вещество, включително от генетични данни и биологични проби; *и всякаква информация, например за заболяване, увреждане, риск от заболяване*, медицинска история, клинично лечение или физиологично или биомедицинско състояние на субекта на данните, независимо от източника на информация, като например лекар или друг медицински специалист, болница, медицинско изделие или ин витро диагностично изследване. Също така съгласно съображение 54 от Регламент 2016/679, обработването на специални категории лични данни може да е необходимо по съображения от обществен интерес в областта на общественото здраве, без съгласието на субекта на данните. Такова обработване следва да бъде предмет на подходящи и конкретни мерки с оглед защита на правата и свободите на физическите лица. *В този контекст понятието „обществено здраве“ следва да се тълкува по*

смисъла на Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета (11) и означава всички елементи, свързани със здравето, а именно здравословно състояние, включително заболеваемост и инвалидност, решаващи фактори, които оказват влияние върху това здравословно състояние, потребности от здравно обслужване, средства, отделени за здравно обслужване, предоставяне на здравни грижи и всеобщ достъп до тях, разходи и финансиране на здравното обслужване, както и причини за смъртност. Такова обработване на данни за здравето по съображения от обществен интерес не следва да води до обработването на лични данни за други цели от трети страни като работодатели или застрахователни дружества и банки. Съгласно съображение 71, пар. 2 членството в синдикални организации също попада в обхвата на специални категории данни. *Освен това в чл. 4, т. 15 от Регламента се дава легална дефиниция на „данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние.* Чл. 9, ал. 1 от Регламента гласи, че се забранява обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице. В съответствие на съюзното право е и разпоредбата на чл. 51 от ЗЗЛД, ал. 1 от която гласи, че обработването на лични данни, разкриващо расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравословното състояние или сексуалния живот и сексуалната ориентация на лицето, е разрешено, когато това е абсолютно необходимо, съществуват подходящи гаранции за правата и свободите на субекта на данни и е предвидено в правото на Европейския съюз или в законодателството на Република България. *Чл. 9, ал. 2, б. „б“ от Регламента гласи, че обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, дотолкова, доколкото това е разрешено от правото на Съюза или правото на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните.* Тази разпоредба е израз на съображение 53 от Регламента, която предвижда, че дерогация от забраната за обработване на специални категории лични данни също следва бъде разрешена, когато е предвидена в правото на Съюза или правото на държава членка, и при подходящи гаранции, така че да бъдат защитени личните данни и други основни права, когато съображения, свързани с обществения интерес, оправдават това, по-специално обработването на лични данни в областта на

трудовото право, правото в областта на социалната закрила, включително пенсиите, както и за целите на сигурността, наблюдението и предупрежденията в сферата на здравеопазването, предотвратяването или контрола на заразните болести и други сериозни заплахи за здравето. Такава дерогация може да се извърши за здравни цели, включително общественото здраве и управлението на здравните услуги, особено с цел да се гарантират качеството и рентабилността на използваните процедури за уреждане на искове за обезщетения и услуги в системата за здравно осигуряване, или за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели. *Чрез дерогация следва да се даде възможност да се обработват и такива лични данни, когато е необходимо, с цел установяване, упражняване или защита на правни претенции, независимо дали това е в рамките на съдебна, административна или друга извънсъдебна процедура*.

Жалбоподателят посочва (л. 594 по делото), че в Закона за данъците върху доходите на физическите лица (ЗДДФЛ) е предвидена възможност лица с 50 или с над 50 на сто намалена работоспособност, както и лица отглеждащи деца с увреждания да ползват данъчни облекчения. Тези обстоятелства се декларират в годишната данъчна декларация по чл. 50 от ЗДДФЛ, който образец се утвърждава със заповед на министъра на финансите (чл. 64, ал. 1 от ЗДДФЛ). *Едва от 01.01.2020 г. при подаване на годишна данъчна декларация отпада необходимостта от представяне пред НАП на решение на ТЕЛК (НЕЛК). Не е необходимо да се вписва и номер на решение*. В НАП обаче постъпват решения на експертни лекарски комисии, съдържащи данни за % на намелена работоспособност и/или противопоказни условия на труд, основани на преценка на комисиите за здравословното състояние на служителите. Решенията се въвеждат в програмен продукт „Х.“ с оглед последващо упражняване на права от страните на посочените в тях служители, включващи право на трудоустрояване по реда на Наредбата за трудоустрояване, полагаем по-висок размер на платен годишен отпуск по смисъла на чл. 56, ал. 2 от Закона за държавния служител, респ. чл. 319 от Кодекса на труда, както и предвидените в ЗДДФЛ данъчни облекчения. Личните данни, които НАП обработва в своите информационни системи, съгласно чл. 72, ал. 1 ДОПК, са включени като част от данъчната и осигурителна информация за задължените лица и процедурите, свързани с обработването на данъчната и осигурителната информация са същите, с които се обработват и личните данни. Това е така, защото предвид естеството на личните данни за задължените субекти в сферата на прилагането на данъчното и осигурителното законодателство, същите се припокриват с данните представляващи и данъчна и осигурителна информация, по смисъла на чл. 72, ал. 1 от ДОПК. Специални категории лични данни по чл. 9 от Регламент 2016/679 се обработват съгласно чл. 9, пар. 2, б. „б“ от Регламент 2016/679, по смисъла на чл. 87, ал. 2, т. 7 от ДОПК като други обстоятелства, свързани с възникване, промяна и погасяване на задълженията за данъци и задължителни осигурителни вноски. Разпоредбата на чл. 87 от ДОПК определя и съдържанието на данъчно-осигурителната информация, която се обработва в НАП за задължените лица. Изпълнителният директор на НАП

утвърждава формата и елементите на данъчно-осигурителната сметка със заповедта по чл. 81, ал. 2 от ДОПК. НАП не обработвала специални категории лични данни съгласно чл. 9 от Регламент 2016/679 за цели извън случаите по чл. 9, пар. 2, б. „б“ за установяване на данъчни и осигурителни задължения, предвид което жалбоподателят счита, че са приложими и се прилагат политиките и процедурите, свързани с обработването на данъчна и осигурителна информация в НАП и не е необходимо да разработва специални правила/процедура, регламентиращи мерките за защита на специалните категории данни, тъй като те се обработват като данъчна и осигурителна информация и са обект на системата за информационна сигурност.

Видно от твърдението на самия жалбоподател, той събира данни за здравословното състояние на лицата, *доколкото всеки процент ТНР е последица от психическо или физическо* увреждане на конкретно лице.*Следва допълнително да се посочи, че данните за намалена работоспособност, както и за лица, отглеждащи деца с увреждания за ползването на данъчни облекчения, са се събирали чрез представяне на решения на ТЕЛК, като се е записвал номера на решението към дата на издаване на оспореното решение на КЗЛД.* Този факт е в съответствие както с посоченото от жалбоподателя, така и констатациите на вещото лице по втората СТЕ, така и с утвърдения регистър на категориите дейности по обработване (л. 355-357). Това обстоятелство попада в хипотезата визирана в съображение 35 от Регламента - „номер, символ или характеристика, определени за дадено физическо лице с цел уникалното му идентифициране за здравни цели“, както и в хипотезата на съображение 54 от Регламента, което касае данни за инвалидност. Данните за намалена работоспособност представят данни за здравословното състояние на лицето по чл. 4, т. 15 от Регламента, което може да бъде основание за дискриминация. Решенията на експертни лекарски комисии, съдържащи данни за % на намелена работоспособност отново следва да се характеризират по същия начин и попадат в приложното поле на съображение 35 и 54 от Регламента, както и по чл. 4, т. 15 от Регламента и с оглед на следващо упражняване на правата от лицата, същото важи и за данни за увреждането, изрично посочени в съображение 35 като данни за здравословно състояние на лицето. Чл. 9, пар. 1 от Регламента установява изрична забрана за обработване на такъв тип данни. В пар. 2 от Регламента са установени изчерпателно изброени изключения от този принцип. В съответствие с чл. 9, пар. 2, б. „б“ от Регламента в ДОПК е предвидена възможност за събиране на такъв тип информация за данъчни и осигурителни цели предвидена в разпоредбата на чл. 87, ал. 2, т. 7. В този смисъл противоречива е самата теза на жалбоподателя, че не събира специални категории лични данни, а от друга, че събира такива данни само за целите на чл. 9, пар. 2, б. „б“ от Регламента. Целта на пар. 2, б. „б“ от Регламента е именно да могат да се събират такива (специални лични) данни в изчерпателно определени хипотези. Не случайно наименованието на чл. 9 е „Обработване на специални категории лични данни“. Целта на Регламента, видно от посочените по-горе съображения, е когато се събират такива лични данни, техният режим да бъде специален,

затова и има изрични изисквания кога може да се събират. С оглед на това, за съда изглежда необосновано твърдението на жалбоподателя, че тези лични данни, които имат толкова засилена регулация и сред които изрично е посочено „здравословно състояние“ в пар. 1, не попадат в режима на специална категория лични данни и за НАП не е необходимо да предвижда специален ред за тяхната защита, като те „се припокриват с данните представляващи и данъчна и осигурителна информация, по смисъла на чл. 72, ал. 1 от ДОПК.“ Тълкуването на член 8, параграф 1 от Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни или на член 9, параграф 1 от Регламент 2016/679 в смисъла вложен от НАП сочи противоречие с целта на посочените разпоредби, а именно да се осигури по-голяма защита по отношение на подобно обработване, което поради особената чувствителност на тези данни може да представлява, както следва и от съображение 33 от тази директива и от съображение 51 от този регламент, особено тежко вмешателство в основните права на зачитане на личния живот и на защита на личните данни, гарантирани от членове 7 и 8 от Хартата на основните права на Европейския съюз. Съдът приема, че именно поради предоставената на национално и на съюзно ниво дерогация от чл. 9, пар. 1 от Регламента, НАП може да събира информация за здравословното състояние на лицата, с оглед упражняването на предвидените права от тези лица. Когато събира и обработва такава информация НАП е длъжна да подхожда с необходимите завишени изисквания към нея, защото тя попада в специалната категория лични данни /чувствителни данни/.

В КА е споменато и събирането на данни относно синдикална принадлежност /л. 157/, като тези данни попадат в приложното поле на чл. 9 от Регламента и тяхното събиране на първо място представлява специална категория лични данни и на второ място то е възможно само в изрично предвидени хипотези по пар. 2. Този факт не е коментиран, но вещото лице по първата СТЕ констатира, че не се събират лични данни съдържащи информация разкриваща членство в синдикални организации, като тази липса е констатирана и във втората СТЕ. Съдът изцяло кредитира заключенията на двете СТЕ в тази част, като в допълнение към тях сочи, че в утвърдения регистър на категориите дейности по обработване (л. 355-357) липсва събирането на такава информация.

С оглед на гореизложеното, съдът приема, че за НАП е възникнало задължение да предвиди специални правила за обработка на един тип специална категория лични данни, а именно здравословно състояние на лицата. Независимо от заключението по втората СТЕ, че Правилата и изкисванията в стандарт БДС ISO/IEC 27001/2014 са по-разширени от изискванията, заложени в Регламент 2016/679 и следва да се приемат за достатъчни при осигуряване на защитата на личните данни, съдът сочи, че не е съобразено обстоятелството, че се обработват специална категория лични данни, което налага конкретна правна регулация, в допълнение и от казаното в о.с.з от вещото лице, този стандарт е само основата на която стъпва Регламентът и надгражда над нея. Възраженията на жалбоподателя свързани

с прекалено широкото формулиране на предвидените предписания следва да се възприеме в смисъл, че на жалбоподателя е предоставена по-широка оперативна самостоятелност за въвеждането на подходящите правила и процедури за обработка на лични данни.
С оглед на изложеното,разпореждания № 3 и № 13 от оспореното решение се определят като съответни на материалния закон.
2. Разпореждане № 1 и Разпореждане № 4 се разглеждат заедно, като отнасящи се до правата на привилегированите потребители, видно от мотивите за приемането на разпорежданията. *Според първата СТЕ, към момента на изследването от ВЛ вече са били взети мерки за въвеждане в активната директория на правила за достъп на отделните групи потребители и привилегированите потребители имат ограничен специализиран достъп до информационните ресурси.* Всеки привилегирован потребител има достъп до определени информационни ресурси, а не до целия информационен ресурс. Този специализиран достъп е ограничен до степен, даваща възможност за изпълнение на служебните задължения на служителите по длъжностна характеристика. Конкретните задължения на привилегированите потребители са определени със заповед на изпълнителния директор на НАП. Коментирана е Заповед ЗЦУ – 585/24.03.2021 г., с утвърдени роли за достъп до информационните системи на НАП, където се обработват и визуализират различен по обхват данни и се създават коректни правила за защита на различните категории лични данни. Съдът приема, че тази заповед, тъй като е след датата на издаване на Решението на КЗЛД не следва да се взема предвид при преценката за законосъобразност. Този факт бил имал значение за изпълнението на разпорежданията, а не за законосъобразността им. *В о.с.з от 04.01.2022 г. вещото лице К. заявява, че няма как да се установи към момента на теча на лични данни, дали тези конкретно мерки са били взети, като в технологичен момент, не е сигурно кога точно е станал течът реално. Много вероятно е да е осъществен по-рано от установяването му и то на няколко пъти.* Според втората СТЕ активната директория е била въведена за всички служители на НАП към 19.07.2019 г., чрез което се осъществява контрол на достъпа и се делегират права на потребителите за достъп до информационните активи. Било е установено, че на 24.03.2021 г. е издадена Заповед ЗЦУ -358, която е последна към момента на изследването от ВЛ, регламентираща утвърдените роли за достъп до Информационни системи на НАП, визуализиращи и обработващи различен по обхват данни. Същата заповед е предхождана от редица други, отменени от нея, като тази предхождаща 15.07.2019 г. е Заповед № 9/ ЗЦУ – 472/01.04.2019 г., приложена към жалбата на НАП по настоящото дело. В о.с.з на 30.05.2022 г. вещото лице В. заявява, че има работеща активна директория. Това е софтуерен механизъм, чрез който се раздават права за достъп на отделните потребители. След внедряване на приложението, разработчиците трябва да имат само сервизен достъп, но към момента на извършване на експертизата не може да каже със сигурност дали това е било така към и към 15.07.2019 г.
Що се отнася до изложеното в о.с.з на 04.01.2022 г., в което вещото лице К. твърди, че е констатирал липса на лична отговорност на служителите, тези

констатации са извън обхвата на настоящия спор, макар и личната отговорност на служителите да е разгледана в КА /л. 156, гръб/, тя не е предмет на дадено с оспореното решение разпореждане.
Безспорно се установява и според двете СТЕ, че към момента на извършване на експертизите има въведена активна директория за правила на достъп на отделните групи потребители и привилегированите потребители имат ограничен специализиран достъп до информационните ресурси. Следва да се посочи обаче, че в първата експертиза, вещо лице не може да твърди със сигурност дали такава активна директория е била създадена към момента на теча, като се има предвид, че е било много вероятно, течът да е станал на няколко пъти. Препращане е направено само към действащата към момента на проверката заповед. Втората СТЕ препраща към заповед от 1.04.2019 г., която е приложена по делото (л. 58-60). Съдът констатира от нея единствено обстоятелството, че с нея е предоставен администраторски достъп на служители до информационни активи и услуги. *От тази заповед обаче, не може да се установи, дали всеки привилегирован потребител има достъп до определени информационни ресурси, а не до целия информационен ресурс, тъй като това обстоятелство следва да бъде установено не от документи, а чрез функционирането на системата и нейното проверяване от лица, със специални знания в областта на информационните технологии и кибер сигурността. На следващо място, вещото лице не е могло да установи дали активната директория е работила към процесната дата и дали разработчиците са имали единствено сервизен достъп. При тези данни и съобразявайки се с обърнатата доказателствена тежест съгласно чл. 59, ал. 1 от ЗЗЛД и чл. 24, § 1 от Общия регламент, съдът приема, за недоказано законосъобразното обработване на данните, разписано като законово задължение на администратора, което обуславя и материалната законосъобразност на разписанията към датата на издаването им. Следва да се посочи още, че що се отнася до принципа P. By D., КЗЛД постановява, че при следващо внедряване на системен продукт, тези мерки следва да бъдат изпълнени на ниво проектиране, а не по отношение до предходни действия на НАП.*
3. Относно разпореждане № 5.
Съгласно първата СТЕ, НАП е разполагала със Система за управление на привилегиите на потребителите (Privileged Access M.), която към 15.07.2019 г. е функционирала в тестова среда, а в момента на изследването от ВЛ вече е напълно внедрена. За привилегированите потребители системни администратори, администратори на приложни сървъри и администратори на база данни има одитни записи за събитията за достъпите им до операционните системи на сървърите и действията им на тях. За привилегированите потребители разработчици на информационни системи, които нямат пряк достъп до операционните системи на сървърите и достъпват информационните системи чрез потребители на базите данни, няма одитни записи за събитията. Към 15.07.2019 г. Агенцията е разполага със система за одитиране и анализ на информационната инфраструктура (QualysGuard), доставена през 2015 г. *Според посочени от служители на данни, в резултат на извършена оценка през 2019 г. на стратегическите*

рискове в НАП е идентифицирана необходимост от придобиване на S. information and event management и са били планирани средства за такава система. Към датата на посещението от ВЛ в НАП, няколко софтуера, които в цялост изграждат такава система са в процес на пускане в експлоатация. В о.с.з на 04.01.2022 г. вещото лице К. сочи, че при посещението му в НАП, като първият път това е било в началото на 2020 г., посочените 3 софтуера на стр. 7 от заключението са били в процес на инсталиране, но няма данни, кога са придобити от НАП. В НАП процесът по придобиване и инсталиране е доста дълъг, защото първо се инсталират в тестова среда, правят се обучения на администратори и чак впоследствие се инсталират в работна среда. Добавя още, че при извършване на изследването е установил два вида технически дневници. Едните от тях касаят базите данни, като те са описани на стр. 8,9 и 10 от заключението. Установени са файлове от 2019 г. от датата на узнаване на теча. Установени са файлове, които са от юни месец 2019 г. и впоследствие от месец юли и август 2019 г. Тези файлове касаят технически обръщения, технически комуникация с базите данни, те не касаят потребителите. На техническо ниво, базата данни е това, което съдържа информацията от системите на НАП, това е основният елемент от тяхната информационна система. НАП притежава няколко сървъра на база данни. Вещото лице е получило достъп до файловете, до тези лог-файлове на сървъра, от който вероятно са изтекли данните. Съществуват лог-файлове за периода от юни 2019 г. до момента на изследването извършено от него, като те са много подробни. В тях има много техническа информация и не са били изследвани подробно от вещото лице. Обяснява още, че е изследвал системата за контрол на потребителите, включително и привилегированите потребители, в която също има данни от 15.07.2019 г., но тогава системата е работила в непълен капацитет, тъй като тя е била все още тестова. Съгласно втората СТЕ за действията на системните администратори, администратори на приложни сървъри и администратори на база данни, потребители на информационни системи, се поддържат записи за достъп до операционните системи и извършените върху тях действия, като генерираните от информационните системи лог-файлове не се трият, а се съхраняват постоянно, такива в случая били съхранявани от преди 2000 г. *Към 15.07.2019 г. НАП е била в процес на внедряване и е разполагала със система за управление привилегиите на потребителите /P. Access M./, работеща в тестова среда, а към настоящия момент е напълно функционална. През 2015 г. е доставена и внедрена Система за одитиране и анализ на информационната инфраструктура /QualysGuard/, функционираща към 15.07.2019 г. Към 15.07.2019 г. НАП не е разполагала с по-долу изброените системи, а непосредствено след инцидента по изтичане на данни е закупила и внедрява следните системи за осигуряване на необходимо ниво на Киберсигурност: - SIEM – софтуер и хардуер за анализ и събиране на журнални събития, DLP – софтуер за предпазване от изтичане на данни, I. and Access M. – софтуер за управление на идентичността и достъпа. От мотивите в заключението е видно, че за потребители разработчици, които нямат пряк достъп до операционните системи на сървърите, не се поддържат записи за събития и извършени*

действия. В о.с.з от 30.05.2022 г. вещото лице В., обяснява, че говори за самите лог-файлове, в които се записват отделните действия на потребители в системите. Записът е автоматизиран процес във всяка информационна система. Въведените по-нови системи, посочени от него в абзац 5, са с цел да се осигури необходимото ниво на киберсигурност.

С оглед на сходството в констатациите по двете СТЕ, съдът приема за установено, на първо място, че разпореждането да се „предприемат необходимите действия за създаване на одитни записи на отделните събития и дневници /журнали/ за привилегированите потребители“ към процесната дата е било изпълнено и такива одитни записи за действията на системните администратори, администратори на приложни сървъри и администратори на база данни, потребители на информационни системи, са били създавани и преди тази дата, като са съхранявани и преди 2000 г. С оглед на това, съдът приема, че в тази му част разпореждане № 5 се явява незаконосъобразно и следва да се отмени.

Относно внедряването на „Система за управление на привилегиите на потребителите /Privileged Access M., PAM/ и Система за управление и анализ на събитията, отразени в дневниците /S. information and event management, SIEM/“. И според двете СТЕ първата система /PAM/ е била внедрена, но на тестово ниво, поради което следва, че не е била напълно функционална. Относно втората система /SIEM/, съгласно втората СТЕ, към 15.07.2019 г. НАП не е разполагала със съответната система, а непосредствено след инцидента по изтичане на данни е закупила и внедрява тази система, заедно с още няколко. Съгласно първата СТЕ същите тези системи към момента на проверката са в процес по внедряване, което потвърждава заключението на първата СТЕ, че към процесната дата тези системи не са били функционали в НАП. Както посочва вещото лице К., в НАП процесът по придобиване и инсталиране е дълъг, защото първо се инсталират в тестова среда, правят се обучения на администратори и чак впоследствие се инсталират в работна среда. Що се отнася до системата QualysGuard, разпореждане за нейното въвеждане не е дадено от КЗЛД, съотв. не е относимо към спора. При тези факти, съдът приема, че разпореждането в посочената част към момента на издаването на Решението на КЗЛД е било необходимо и съответно на дължимото поведение от страна на жалбаподателя-НАП.

4. Разпореждане № 6, 7, 8, 9, 10 се разглеждат в съвкупност, тъй като се отнасят до оценка и управление на риска, както и до въвеждане на нови системи. С първата СТЕ се установява, че „Методика за управление на риска“ и процедура „Оценка на риска за информационната сигурност“, утвърдени от изпълнителния директор на НАП, са базирани на схващането, че всяка една информационна система на НАП, съдържа нормативно защитена информация (лични данни, данъчна и осигурителна информация и др.) и не са изготвяли отделни правила за всяка система, а анализ за риска за всички системи се е извършвал в рамките на общата оценка на риска за информационните активи. Не е извършван отделен/самостоятелен анализ на системите и операциите по обработване. Според посочените от служителите данни, анализът на риска, свързан с информационните активи, се е извършвал регулярно по ред утвърден от изпълнителния директор на НАП. Оценката и управлението на

риска са се извършвали съгласно утвърдени в НАП процедура и Методика за оценка на риска за информационната сигурност и посочени следните допълнителни мерки: Всички служители са подписали декларации по чл. 14, ал. 3 от Закона за Националната агенция за приходите (ЗНАП) и чл. 61, ал. 1 от Закона за защита на личните данни (ЗЗЛД) (Приложение № 1 към чл. 24, ал. 2 към Инструкция № 2 от 08.05.2019 г. за мерките и средства за защита на лични данни, обработвани в НАП и реда за движение на преписки и заявяване на регистри), както и са включени специални изисквания в длъжностните характеристики на служителите. Към момента на разработването на информационните системи в НАП изискванията на Регламент 2016/679 за оценка на въздействие (риска) не са били действащи, поради влизането му в сила през месец май 2018 г. Служителите на НАП са посочили, че след влизане в сила на Регламент 2016/679 в НАП не са въвеждани нови технологии, при които, преди да бъде извършено обработването съобразно естеството, обхвата, контекста и целите на обработването, да се породи „висок риск за правата и свободите на физическите лица“. Следователно не била възникнала необходимост от извършване оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. Съгласно утвърдените в НАП процедури и методика за оценка на риска за информационната сигурност, в дирекциите в които се въвежда управлението на нови информационни системи и приложения се извършва оценка на риска, като се анализират заплахите за информационната система заедно с потенциалните уязвимости и съществуващи мерки. По отношение на принципа „P. By D.“, по време на срещите е било посочено, че тълкуването на НАП е, че на основание чл. 25 от Регламент 2016/679 за администраторите на лични данни произтича като задължение считано от 25.05.2018 г., където на етап проектиране на информационни системи, следва да се осигуряват неприкосновеност и защита на личните данни. В тази връзка, в периода 25.05.2018 г. – 15.07.2019 г. НАП не била разработвала или внедрявала нова информационна система или услуга.

С втората СТЕ се установява, че съществува „Методика за управление на риска“, както и „Оценка на риска за информационната сигурност“, съобразени с изкисванията на стандарт БДС ISO/IEC 27001/2014 и утвърдени със заповед на изпълнителния директор на НАП. Спрямо чл. 35 от Регламент 2016/679 тези правила са съпоставими и следва да се приеме, че отговарят общо на изискванията. Тези правила са приложими за всяка една информационна система, притежавана и използвана от НАП от момента на нейното първоначално въвеждане в експлоатация и според тях са извършвани последващи периодични оценки на рисковете за отделните системи. Не се събирали специална категория лични данни и не се извършват действия и операции по чл. 35 от Регламент 2016/679. В периода м. януари – м. април 2018 г. е имало сформирани две вътрешни групи за преглед и адаптиране на информационните системи и правилата и политиките на НАП за защита на информацията спрямо изискванията на Регламент 2016/679, като в част от системите и начините за предаване на данни към системите на други институции, там където е било възможно, са били взети мерки за анонимизиране и минимизиране на данните. В о.с.з. на 30.05.2022 г. вещото

лице В. пояснява, че като е казал, че според тях са извършени последващи периодични оценки на рисковете, е искал да каже, че той се е запознал с анализите, които са правени за оценка на риска. Веднъж годишно са правени анализи. Уточнява, че И. стандарта е международен стандарт за информационна сигурност. В него се дават най-общите минимални правила, които следва да спазва всяка една организация, като след това развитието на Регламент 2016/679 в частта за осигуряване на информационната сигурност, също стъпва върху този признат международен стандарт.
Преди да се отговори по съществото за спазването на материалноправните разпоредби, следва отново да бъде разгледани приложимите съюзни разпоредби. Чл. 35, пар. 1 от Регламент 2016/679 гласи, че Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове. Чл. 35, пар. 3, б. „б“ от Регламента гласи, че Оценката на въздействието върху защитата на данните, посочена в параграф 1, се изисква по-специално в случай че мащабно обработване на специални категории данни, посочени в член 9, параграф 1 или на лични данни за присъди и нарушения по член 10 Разпоредбата на чл. 35, пар. 4 от Регламента постановява, че Н. орган съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно параграф 1. Н. орган съобщава тези списъци на Комитета, посочен в член 68. Съгласно съображение 85 от Регламента, за да се подобри спазването на настоящия регламент, когато има вероятност операциите по обработването да доведат до висок риск за правата и свободите на физическите лица, администраторът следва да отговаря за изготвянето на оценка на въздействието върху защитата на личните данни, за да се оценят по-специално произходът, естеството, спецификата и степента на този риск. Резултатите от оценката следва да бъдат взети предвид, когато се определят съответните мерки, за да се докаже, че обработването на лични данни отговаря на изискванията на настоящия регламент. Когато в оценка на въздействието върху защитата на личните данни е указано, че операциите по обработването водят до висок риск, който администраторът не може да ограничи с подходящи мерки от гледна точка на налични технологии и разходи за прилагане, преди обработването следва да се осъществи консултация с надзорния орган. В допълнение съображение 89, 90 и 91 от Регламента постановяват, че в Директива 95/46/ЕО се предвижда общо задължение за уведомяване на надзорните органи относно обработването на лични данни. Това задължение създава административна и финансова тежест и невинаги е допринасяло за подобряването на защитата на личните данни. Ето защо такива неправещи разграничения общи задължения за уведомяване следва да бъдат премахнати и заменени с ефективни процедури и механизми, които да са насочени към онези видове операции по обработване, които има

вероятност да доведат до висок риск за правата и свободите на физическите лица поради своето естество, обхват, контекст и цели. Такива могат да бъдат операциите по обработване, които по-конкретно включват използването на нови технологии или представляват нов вид технологии и при които преди това от администратора не е извършвана оценка на въздействието върху защитата на данните или които стават необходими предвид времето, изминало от първоначалното обработване. *В такива случаи, преди обработването администраторът следва да извърши оценка на въздействието върху защитата на данните, за да се оценят конкретната вероятност и тежестта на високия риск, като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска. Посочената оценка на въздействието следва да включва по-специално предвидените мерки, гаранции и механизми за ограничаване на този риск, с които се осигурява защитата на личните данни и се доказва съответствието с настоящия регламент.* Това *следва да се прилага по-специално за широкомащабни операции по обработване, чиято цел е обработване на значителен обем лични данни на регионално, национално и наднационално равнище, които биха могли да засегнат голям брой субекти на данни и които е вероятно да доведат до висок риск, например поради чувствителното си естество, когато в съответствие с постигнатото ниво на технически познания се използва нова технология в голям мащаб,* както и за други операции по обработване, които пораждат висок риск за правата и свободите на субектите на данни, по-специално когато тези операции затрудняват субектите на данни да упражняват правата си. Оценка на въздействието върху защитата на данни следва да се извършва и когато личните данни се обработват с цел вземане на решения относно конкретни физически лица след систематична и обстойна оценка на личните аспекти, свързани с физически лица, въз основа на профилирането на тези данни или след обработването на специални категории лични данни, биометрични данни или данни за присъди и нарушения или свързани с това мерки за сигурност. *Чл. 25, пар. 1 от Регламента гласи, 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. Свързаното с този член съображение 78 от Регламента, предвижда, че защитата на правата и свободите на физическите лица с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира изпълнението на изискванията на настоящия регламент. За да*

може да докаже съответствието с настоящия регламент, администраторът следва да приеме вътрешни политики и да приложи мерки, които отговарят по-специално на принципите за защита на данните на етапа на проектирането и защита на данните по подразбиране. Такива мерки могат да се изразяват, inter alia, в свеждане до минимум на обработването на лични данни, псевдонимизиране на лични данни на възможно най-ранен етап, прозрачност по отношение на функциите и обработването на лични данни, създаване на възможност за субекта на данни да наблюдава обработването на данни, възможност за администратора да създава и подобрява елементите на сигурността. При разработването, проектирането, подбора и използването на приложения, услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, за да изпълнят функцията си, производителите на продукти, услуги и приложения следва да бъдат насърчавани да вземат предвид правото на защита на лични данни при разработването и проектирането на такива продукти, услуги и приложения и като отчитат надлежно достиженията на техническия прогрес, да се уверят, че администраторите и обработващите лични данни са в състояние да изпълняват своите задължения за защита на данните. Принципите на защита на данните на етапа на проектирането и по подразбиране следва да се вземат предвид и в контекста на процедурите за възлагане на обществени поръчки.

Следва отново да се посочи и приетото от съда в т. 1 от мотивите по материалната законосъобразност на разпореждания № 3 и № 13, че НАП обработва специална категория лични данни, а именно данни свързани със здравословното състояние на лицата и поради това чл. 35, пар. 3, б. „б“ е приложим в настоящия случай, с оглед обработването на данни по чл. 9 от Регламента от страна на НАП, поради което констатациите на СТЕ и аргументите на жалбоподателя се отхвърлят. *По съществото, разпорежданията свързани с оценка на въздействие върху защитата на данни визирани в чл. 35 от Регламента и съотносимите към него съображения, цитирани по-горе, следват да се тълкуват в смисъл, че оценка на въздействието върху защитата на данните е необходима винаги когато съществува висок риск за правата и свободите на физическите лица, а не само при въвеждането на нова технология.* По-*специално това се отнася когато преди това от администратора не е извършвана оценка на въздействието върху защитата на данните или които стават необходими предвид времето, изминало от първоначалното обработване. Също така пряко относимо към обработването от НАП е и следната част от съображенията на Регламента „широкомащабни операции по обработване, чиято цел е обработване на значителен обем лични данни на регионално, национално и наднационално равнище, които биха могли да засегнат голям брой субекти на данни и които е вероятно да доведат до висок риск, например поради чувствителното си естество“. Безспорен факт е, че НАП извършва широкомащабни операции по обработване на лични данни на българските и чужди граждани. А. на НАП, че „след влизане в сила на Регламент 2016/679, в НАП не са въвеждани нови технологии, при които преди да бъде извършено обработването, предвид естеството, обхвата,*

контекста и целите на обработването да се породи „висок риск за правата и свободите на физическите лица“ и да възникне необходимост от извършване оценка на въздействието на предвидените операции по обработването върху защитата на личните данни“, показва неоснователно смесване на две разпоредби- тази на чл. 25 от Регламента и тази на чл. 35 от Регламента. В анализа за оценка за въздействие, чл. 25 от Регламента не намира приложение и следователно е без значение дали има въведени нови технологии или не. Тълкуването от страна на НАП на чл. 35 от Регламента с изключителен акцент върху думите „нови технологии“ като се приема от тяхна страна, че тази разпоредба е приложима само когато се използват нови технологии, противоречи на частите на изречението в граматичен аспект. Фразата „по-специално при което се използват нови технологии“ е подчинено изречение на главното и посочва само един пример кога с по-голяма основателност следва да се извърши оценка на въздействието върху защитата на данните, а не че само тогава и единствено тогава следва да се извърши. Освен това съгласно Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка на въздействието върху защитата на данните съгласно чл. 35, пар. 4 от Регламент 2016/679, представен по делото като доказателство от жалбоподателя /л. 55/, Раздел II /който касае видовете операции/, т. 3 гласи, че обработване на данни за местоположение с цел профилиране, което поражда правни последици за субекта на данни или по подобен начин го засяга в значителна степен. В случая се установява, че в регистъра с категориите дейности по обработване от НАП /л. 355-357/ за почти всички категории дейности се събират лични данни за адрес. Думите адрес и местоположение са различни, но тяхното съдържание е сходно. Съгласно Тълковен речник на Б., местоположение означава: "Място, където е разположено селище, сграда или под., обикн. всред някакви природни особености; месторазположение, местонахождение". Думата адрес, пак според Тълковния речник на Б., означава: "Данни, указание за местонахождението и името на лице, учреждение и др., написани върху плик, телеграма, колет и др., до които се изпращат". По тези съображения съдът приема, че НАП не е изпълнила изискването за оценка на въздействието свързано с обработването на информация, която касае местоположението на лицата. С оглед на тези съображения, съдът приема, че в тази си част разпорежданията са съгласувани с материалноправните основания и чл. 35 от Регламента намира приложение.

Конкретно относно разпореждане № 7, съдът сочи, че съгласното и двете СТЕ, анализът на риска, свързан с информационните активи, се е извършвал регулярно по ред утвърден от изпълнителния директор на НАП, като правилата отговаряли общо на изискванията. В съответствие с това съдът приема, че това разпореждане е лишено от предмет към момента на издаването му и следва да се отмени.

Не е част от правния спор, предмет на делото и въпросът дали извършваните одити са били правени от независим одитор, както и неговата техническа компетентност в областта на защита на личните данни, поради това съдът няма да разглежда този въпрос, коментиран от вещите лица. Това се

обуславя и от обстоятелството, че в КА като мотиви е посочено само липсата за проведени оценки на риска, без да е обсъждана тяхната компетентност, достоверност и изчерпателност. Не е давано и предписание в тази насока.
Относно правилата и процедури при първоначално стартиране на нови информационни системи и приложения, по делото се установява, че НАП не е разработвала или внедрявала нова информационна система или услуга за периода 25.05.2018 г. – 15.07.2019 г. Следва да се отбележи обаче, че КЗЛД не твърди обратното в оспореното пред съда решение. Според КЗЛД, НАП нямат изградени правила и процедури при първоначално стартиране на нови информационни системи и приложения съгласно чл. 25 от Регламента, а не че са разработили или внедрили нова информационна система или услуга без да са спазени тези правила. Разпорежданията са с оглед създаване на правила при бъдещо въвеждане на нова информационна система или услуга. НАП не представя доказателства и не установява наличието на такива правила, като такива не са установени и от вещите лица. Що се отнася до P. By Redesign и P. By Default , жалбоподателят също не оспорва липсата им и не представя доказателства за създаването на такива системи, а вещите лица не са коментирали тези две системи.
При тези обективни данни по делото съдът приема, че разпорежданията свързани с тези предписания са законосъобразни, поади което се отменя само Разпореждане №7.
5. Разпореждане № 11.
Съгласно първата експертиза, към момента на извършване на изследването от ВЛ операционните системи от W. 2008R2 са модернизирани към актуална версия от 2013г. и 2016 г., както и на СУБД O. 11.2.0.2 към актуална версия O. 12. Не е било изцяло обновявано системното и базово програмно осигуряване, защото част от приложните системи не било възможно да работят с по-новите версии на операционната система MS W. и на СУБД O. 11.2.0.2, необходимо е време да се модифицират, а също и допълнително при внедряване на всяка по-нова версия, трябва да се извършва тестване и анализ, с цел установяване работоспособност и непрекъсваемост на системите. До същата констатация стига и вещото лице по втората СТЕ. В третата СТЕ се установява, че системите, от които е извършено източване на данни, са сървъри с операционна система W. 2008R2 и база данни O. 11.2.0.2. Жалбоподателят-НАП, не оспорва, че е прилагала по-стара версия на W. 2008R2 и на СУБД O. към момента на издаване на решението на КЗЛД. Оплакването на администратора НАП е само относно срока, който е предвиден за въвеждането на новите системи (тяхното обновяване). Видно и от двете СТЕ, НАП е в процес по обновяване на системи, но това е бавен процес с оглед осигуряването функционирането на приложните системи. Дали обаче срокът е достатъчен е въпрос относим при преценката на законосъобразността на последващи санкицонни мерки, ако бъдат предприети от КЗЛД, а отделно от това предвид времетраенето на съдебното производство, към настоящия момент / и преди влизането в сила на оспореното решение/ е изтекъл значително голям период от време.
6. Разпореждане № 12.
Съгласно първата СТЕ, НАП разполага с център за съхраняване на данни,

който се използва за съхраняване на информацията от основните информационни системи на НАП, включително и личните данни обработвани в агенцията. Същият осигурява възстановяване на работата на системите в НАП в сроковете, съгласно Плана за непрекъснатостта на действие на НАП. По отношение на изграждането на центъра за възстановяване на работоспособността на системите в реално време (D. R. C.), който да поддържа пълна функционалност за информационните системи и услуги на НАП в реално време, Агенцията е предприела организационни мерки, като един от вариантите е изграждането на общ център за съхраняване на данни за структурите в държавната администрация под управлението на ДАЕУ. Съгласно втората СТЕ, НАП разполага с D. R. C. за съхранение на данни, който се използва за съхранение на информацията от основните информационни системи на НАП, включително и лични данни обработвани в НАП. Същият осигурява възстановяването на работата на системите в НАП в сроковете, съгласно Плана за непрекъснатостта на дейността на НАП, като синхронизацията на данните се извършва на 2 минути, а при отпадане на критични услуги на основните сървъри, дейността се прехвърля към резервните сървъри. Видно от жалбата, НАП не оспорва липсата на изграждането на център за възстановяване работоспособността на системите в реално време, а предоставения срок от 6-месеца за това. С оглед на тези обстоятелства, следва да се приеме, че разпореждането е законосъобразно, катопо отношение на срока следва да се подчертае, че към момента на изготвяне на експертизите НАП вече е изпълнила предписанието за изграждането на център за възстановяване работоспособността на системите в реално време.

7. Разпореждания № 14,15,16 и 17 се разглеждат заедно, тъй като се отнасят до обработката на данни и съхранението на архиви.

Първата СТЕ не се произнася по този въпрос. Във втората СТЕ е установено, че според вещото лице, няма изрична необходимост да се унищожават електронни данни. Установена е съществуваща и утвърдена процедура от изпълнителния директор на НАП, относно действия по премахване на създадена информация в информационните системи на НАП по повод постъпили искания или с цел осигуряване на работоспособността на системите на НАП. Криптиране на данни не се извършва, освен в случаите, когато това се отнася до данни за вход в информационните системи и при обмен на данни с институциите от ЕС.

На първо място относно повторното използване на личните данни на субектите /Разпореждане 14/, следва да се посочи, че в Регламент 2016/679 и в ЗЗЛД липсват правни норми, които да регулират необходимостта и основанията за създаването на специални права за повторното използване на личните данни на субектите. В КА на КЗЛД се установява само липсата на правила за повторното използване на личните данни, но не се сочи необходимост за създаването на такива правила от от НАП. Както се посочва от жалбоподателя в писмените бележки от 01.09.2022 г., процесът на обработване на лични данни на субектите на данни не следва да се разделя на етапи на обработване, а е цялостен процес и в този смисъл изготвяне на отделна политика за повторно използване на личните данни на субектите на

данни е нецелесъобразно (стр. 19 от 22) . Тази аргументация се споделя и от съда. С оглед на липсата на нормативно изискване и липсата на мотиви за така даденото разпореждане, вкл. и в КА, асоцииран към оспореното решение, същото се явява процесуално и материално незаконосъобразно и следва да се отмени.
На второ място относно анонимизиране, архивиране и унищожаване на електронните данни, използвани еднократно /Разпореждане №15/, вещото сочи, че няма изрична необходимост да се унищожават електронни данни. Този извод противоречи, на чл. 25а от ЗЗЛД, който сочи, че когато лични данни са предоставени от субекта на данни на администратор или обработващ лични данни без правно основание по чл. 6, параграф 1 от Регламент (ЕС) 2016/679 или в противоречие с принципите по чл. 5 от същия регламент, в срок един месец от узнаването администраторът или обработващият лични данни ги връща, а ако това е невъзможно или изисква несъразмерно големи усилия, ги изтрива или унищожава. Изтриването и унищожаването се документират. Също така съгласно чл. 25к от ЗЗЛД работодател или орган по назначаването, в качеството си на администратор на лични данни, определя срок за съхранение на лични данни на участници в процедури по набиране и подбор на персонала, който не може да е по-дълъг от 6 месеца, освен ако кандидатът е дал своето съгласие за съхранение за по-дълъг срок. След изтичането на този срок работодателят или органът по назначаването изтрива или унищожава съхраняваните документи с лични данни, освен ако специален закон предвижда друго. С оглед на горните разпоредби следва да има предвидена възможност за унищожаване на лични данни в предвидени хипотези и процедура за извършване на тази обработка на лични данни. Следва да се посочи и това, че съгласно чл.4, т.2 от Регламента „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. В случая ВЛ констатират утвърдена и съществуваща процедура относно действия по премахване на създадена информация в информационните системи на НАП по повод постъпили искания или с цел осигуряване на работоспособността на системите на НАП. Видно от доказателствата по делото съществуват: 1) Указания за унищожаване на информация и информационни носители в НАП, утвърдени със Заповед № ЗЦУ – 1596 от 29.11.2017 г. на изпълнителния директор на НАП /л.115-129/ и 2) Методика за анонимизиране на индивидуални данни, утвърдена със Заповед № ЗЦУ-121 от 30.01.2017 г. на изпълнителния директор на НАП /л.78-109/ и 3) Вътрешни правила за защита на личните данни на лицата, подаващи сигнали в НАП, утвърдена със Заповед № ЗЦУ-174/10.02.2017 г. на изпълнителя директор на НАП и по конкретно чл. 9 /л. 110-113/. С оглед на тези обстоятелства, съдът приема, че към процесната дата НАП е изпълнила изискванията, които касаят унищожаване и анонимизиране на лични данни. Следва да се отбележи, че в СТЕ не е

обсъдено дали има процедури за архивиране на данни и работа с такива данни. Видно от доказателствата по делото, съществуват Вътрешни правила за оборот на електронни документи и документи на хартиен носител в НАП, утвърдени със Заповед №ЗЦУ-535 от 11.05.2016 г. на изпълнителния директор на НАП /л.130-146/ и по конкретно в Глава пета. Поради това следва да се приеме, че НАП е изработила правила за архивиране на данни към процесната дата. В допълнение трябва да се посочи, че съдът не намира необходимост от изрично въвеждането на нови правила за анонимизиране, архивиране и унищожаване на електронните данни, използвани еднократно. Съдът зачита принципа на оперативната самостоятелност на КЗЛД при осъществяване на правомощията й, но отбелязва, че липсват конкретни мотиви, които да налагат подобно разделяне на процесите извършвани от НАП, тъй като в КА само е посочено, че липсват правила, без да е отбелязана необходимост от съществуването на такива правила. Така установените пороци на акта в тази му част обуславят отмяната му като процесуално и материално незаконосъобразен.

На трето място относно лични данни на деца и повторното използване на такива данни. СТЕ не е разгледала този въпрос. В жалбата също не е оспорено обстоятелството за липса на такива правила и процедури. В писмените бележки на жалбоподателя от 01.09.2022 г. се сочи, че към момента на депозирането им НАП е в процес на изготвяне на такива правила и процедури. Приложимите материалноправни разпоредби към това разпореждане се намират в Регламент 2016/679. Съгласно съображение 38 от Регламента на децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни. Тази специална защита следва да се прилага по-специално за използването на лични данни на деца за целите на маркетинга или за създаване на личностни или потребителски профили и събирането на лични данни по отношение на деца при ползване на услуги, предоставяни пряко на деца. Съгласието на носещия родителска отговорност не следва да е необходимо в контекста на пряко предлаганите на деца услуги за превенция и консултиране. Чл. 57, пар. 1, б. „б“ гласи, че без да се засягат останалите задачи, определени с настоящия регламент, на своята територия всеки надзорен орган: насърчава обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработването. Обръща се специално внимание на дейностите, специално насочени към децата. Съдът приема, че необходимостта от специални правила при обработката на лични данни на деца, визирани в разпореждането е налице, с оглед постигане на целите на Регламент 2016/679, и приема, че това разпореждане е законосъобразно, с изключение на частта, касаеща "повторното използване на такива данни" по вече изложените от съда съображения във връзка с Разпореждане №5.

Относно стратегия и политики за криптиране на данни от архивни или еднократни извършвани справки /Разпореждане №17/, следва да се посочи, че с жалбата не се оспорва липсата на такава политика. Вещото лице по втората СТЕ е установило, че криптиране на данни не се извършва, освен в случаите,

когато това се отнася до данни за вход в информационните системи и при обмен на данни с институциите от ЕС. Материалноправното основание за въвеждането на такава процедура се намира в съображение 83 от Регламента, съгласно което 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. Също така чл. 32, пар. 1, б. „а“ от Регламента гласи, че 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. С оглед недоказаното наличие на такива правила, съдът приема, че това разпореждане е законосъобразно.

8. Разпореждания № 18 и 19 се разглеждат заедно, защото се отнасят до длъжностните характеристики на служителите.

От 01.09.2010 г. с РМФ-56/28.09.2010 г. е одобрена организационно-управленска структура на ЦУ на НАП, с което е създадена дирекция „Превенция на финансовата и информационната система“ на пряко подчинение на изпълнителния директор. През 2015 г. с Решение №-93/24.08.2015 г. на УС в НАП е одобрена нова организационно-управленска структура на Агенцията като считано от 25.08.2015 г. съществуващата дирекция е закрита и е създаден отдел „Превенция на финансовата и информационната система“ в състава на Инспектората на НАП, който е на пряко подчинение на изпълнителния директор и в него има определени служители и административно звено, отговарящо за мрежовата и информационната сигурност. Функциите им са в съответствие с тези, описани в Приложение № 2 към чл. 28, ал. 3 от НОИОСИС. Считано от 01.08.2019 г., е обособена нова дирекция „Мрежова и информационна сигурност на системите“, пряко подчинена на изпълнителния директор на НАП. Към 15.07.2019 г. длъжностното лице по защита на данните в ЦУ на НАП е от отдел „Вътрешна сигурност и защита на информацията“, дирекция „Сигурност“, която е пряко подчинена на изпълнителния директор на НАП. В организационно-управленската структура на ЦУ на НАП с РМФ-56/28.09.2010

г. е създадена дирекция „Превенция на финансовата и информационната система“, която е на пряко подчинение на изпълнителния директор. Същата дирекция е трансформирана с Решение №93/24.08.2015 г. в отдел „Превенция на финансовата и информационната система“ към Инспектората на НАП и в него има определени служители и административно звено, отговарящо за мрежовата и информационната сигурност. Разпоредбата на чл. 38, пар. 3 от Регламента предвижда, че администраторът и обработващият лични данни правят необходимото длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на тези задачи. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни. *Видно от мотивите на КА, двете разпореждания са насочени към това да бъде описано в длъжностите характеристики на лицата, че обработват лични данни.* С оглед на разпореденото, предложените от жалбоподателя аргументи са неотносими. В разпореждане № 18 е поставено и допълнително изискване, относимо само към длъжностното лице по защита на данните. По делото се установява, че това лице е от отдел „Вътрешна сигурност и защита на информацията“, дирекция „Сигурност“, пряко подчинена на изпълнителния директор на НАП. В тази връзка от представените доказателства, а именно четирите броя длъжностни характеристики, относима е само тази свързана със старши експерт главен експерт, отдел ВСЗИ, дирекция „Сигурност“ /л. 239-240/. В нея изрично е записано, че той е подчинен на началника на отдел ВСЗИ. С оглед на тези обстоятелства, съдът намира, че в тази му част разпореждането е законосъобразно, защото НАП не е изпълнила задължението по регламент длъжностното лице по защита на данните да се отчита пред изпълнителния директор на НАП, тъй като попада в хипотезата на „най-висшето ръководно ниво на администратора или обработващия лични данни.“ Що се касае до това да се предвидят ясни права и задължения, видно от длъжностната характеристика има разписани правила за защита на лични данни от длъжностното лице, но те не отговарят дори и на минималните изисквания за длъжността предвидени в чл. 39 от Регламент 2016/679, като нито една от петте задачи визирани в тази разпоредба не е посочена конкретно в длъжностната му характеристика. При тези данни се налага извод, че разпореждането е законосъобразно.

9. Разпореждания № 2 и 20 се разглеждат заедно, защото касаят обучението на служителите, от една страна, а от друга- техническите и организационни мерки с цел повишаване защитата на лични данни. Първата СТЕ установява, че към датата на изследването НАП е имала утвърден План за непрекъсваемост на дейността и планове за непрекъсваемост на критичните информационни системи. Също така има утвърдена процедура, която описва действията на служителите от НАП при съмнения за инцидент, касаещ информационната сигурност и специфичните дейности, които извършват служителите от отдел „Превенция на финансовата и информационната система“ при Инспекторат на НАП и сектор “Help desk център“ при дирекция

„Информационни системи и моделиране на бизнес процесите“ при получен сигнал за инцидент, касаещ информационната сигурност на НАП. Служителите на НАП са участвали в тренировки за симулиране действия при инциденти, свързани с работата на информационните системи в НАП, което респективно засяга и неправомерното обработване на лични данни в НАП, като неразделна част от защитата на данъчната и осигурителна информация. Последното известно участие в подобно обучение е през месец април 2019 г. В о.с.з от 04.01.2022 г. при изслушването му, вещото лице К. пояснява, че липсват обучения за защита на личните данни на целия състав на служители (работещи в НАП). Единственият договор е с Информационно обслужване и Лабораторията за киберсигурност. Обучението за сигурност на данните касаело само малка група от служителите на НАП, т.е касае частично обучение. Изразява съмнения в знанията и техническите възможности на двата субекта. Заявява, че НАП имат и други договори с Информационно обслужване относно аспекти на сигурността на компютърните системи. Смята, че не е редно в чисто технически аспект едни и същи лица да бъдат ангажирани в процесите по инсталиране, експлоатация и обучение, защото така се изкривява процеса, като се представят едни и същи практики и по тази причина е препоръчително да има независим одит. Заявява, че НАП не е изискала помощ от компетентни органи, за да определят дали нивото на мерките е достатъчно, както и нямат независим одит. Според експертното му мнение, при използване на тези практики защитата със сигурност е щяла да е на доста по-високо ниво. Според него в НАП са липсвали адекватни мерки. Съгласно втората СТЕ, НАП разполага с План за непрекъсваемост на дейността и планове за непрекъсваемост на критичните информационни системи, базиран на разработена и внедрена С. по стандарт БДС ISO/IEC 27001/2014. Има разработени и внедрени процедури за действие при настъпили инциденти или при наличие на съмнения при тях. НАП провежда по план обучения на служителите си, най-малко веднъж годишно, относно осигуряване на информационната сигурност на активите и данните, събирани, съхранявани и обработвани от НАП, като е проведено през април 2019 г. В о.с.з на 30.05.2022 г., вещото лице В. пояснява при изслушването му , че като е изложил в заключението, че защитата от нерегламентиран достъп е поета от „Информационно обслужване“ АД от юли 2019 г., е имал предвид времето след 15.07.2019 г., т.е след теча на лични данни. Относно проведеното обучение през април 2019 г. на служители на НАП, сочи, че това касаело служители, които отговарят за информационната система, т.е за служителите на IT отдела, но със информационната система работят всички служители на НАП, както и различни външни потребители. ВЛ изразява експертно мнение, че за последните то не е било необходимо, тъй като обикновените служители работещи в системата на НАП едва ли могат да разберат, ако има нерегламентиран достъп. Съгласно третата СТЕ, когато се говори за осигуряване на защита на информацията не следва да има позоваване единствено на технически мерки, а те следва да бъдат разглеждани комплексно с предприетите организационни такива. Всяка организация е необходимо да изгради собствена С., включваща политики, правила и конкретни инструкции за осигуряване на Информационната сигурност,

базирано на Оценка на риска, направено на базата на конкретните процеси и информационни активи. Една такава С. следва да бъде непрекъснато обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност. Към момента на теча, НАП е имала разработена и внедрена С., изградена върху основни правила, базирани на стандарта за информационна сигурност БДС ISO/IEC 27001/2006 и в последствие актуализирана към по-новата версия БДС ISO/IEC 27001/2014. *На база С. са били определени и изпълнени преценените към онзи момент необходими и достатъчни технически и организационни мерки за защита на информацията, но явно е пропуснато да бъде тествано конкретното приложение за атаки от типа „S. инжекция“ при въвеждането му в експлоатация, както и не е бил извършаван последващ контрол на сигурността на засегнатото W. приложение. „S. инжекция“ е идентифициран като критична заплаха за сигурността минимум от 2007 година, когато излиза първата OWASP Top 10 Vulnerabilities L.. Големият риск от подобен тип атаки се дължи на лекотата, с която могат да бъдат засечени уязвимостите, както и лекотата, с която могат да бъдат експлоатирани тези уязвимости, за да компрометират сигурността на информацията. Вещото лице заявява, че експертизата му позволява да твърди, че технически е било възможно предотвратяването на изтичане на данни към онзи момент-2019 година.*

Съдът намира, че от заключенията по първите две СТЕ се установява, че част от служителите са участвали на обучения, като това са били служители, които отговарят за информационната система, т.е за служителите на IT отдела. Съгласно разпореждане № 20 и мотивите към него, КЗЛД не отрича факта на провеждането на обучения, а само липсата процедура и вътрешни правила за тяхното провеждане. Жалбоподателят НАП не представи доказателства за съществуването на вътрешни правила, а само договори за извършване на подобно обучение.

Съдът приема, че с оглед огромното количество събиране на лични данни на национално ниво, НАП следва да регламентира на вътрешно ниво процедури за обучение на персонала, за да може да се осигури правна сигурност и предвидимост в подготовката на служителите. Въпросът за компетентността на провеждащите обученията обаче не е част от настоящия спор, поради което съдът няма да го разглежда.

Въз основа на изложеното, съдът приема, че разпореждане №20 се явява законосъобразно.

В заключение по делото съдът сочи, че по отношение предприетите технически и организационни мерки, заключенията на вещите лица и по трите СТЕ позволяват да се установи бездействие по смисъла на разпоредбата на чл. 24 "Отговорност на администратора", като не са взети предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, изразяващо с в невъвеждането от администратора на подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с регламента. *Не са предприети предвидените в чл. 32, в) от Общия регламент конкретни мерки, а именно*

не са взети предвид достиженията на техническия прогрес, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица и не са приложени подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно: процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването. В случая въведената система не е била обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност. „S. инжекция“ е била идентифицирана като критична заплаха за сигурността минимум от 2007 година, когато излиза първата OWASP Top 10 Vulnerabilities L. Големият риск от подобен тип атаки се дължи на лекотата, с която могат да бъдат засечени уязвимостите, както и лекотата, с която могат да бъдат експлоатирани тези уязвимости, за да компрометират сигурността на информацията. При редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки, е било технически възможно предотвратяването на изтичане на данни към 2019 година. Администраторът на лични данни по см. на чл. 4 § 7 от Регламента и при обработване на личните данни, не е спазил принципите за законосъобразност и добросъвестност, залегнали в чл. 5 § 1 б. "а", както и по б. "е" от Общия регламент, а именно не е гарантирал подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като не е приложил подходящи техническите и организационни мерки /"цялостност и поверителност"/. И двете вещи лица по трите СТЕ със сигурност твърдят, че изтичането на данни е могло да бъде избегнато, ако са били взети необходимите технически и организационни мерки.

Относно 6-месечния срок за изпълнения на разпорежданията, съдът съобразява констатациите на вещите лице, че в НАП процесът по придобиване и инсталиране е доста дълъг, защото първо се инсталират в тестова среда, правят се обучения на администратори и чак впоследствие се инсталират в работна среда. Съдът обаче вече посочи, срокът не е свързан със законосъобразността на оспорения акт, а с неговото изпълнение и това възражение би могло да се релевира в друго производство-при ангажиране отговорността на НАП за неизпълнение на предписанията. Отделно от това съвсем не е без значение и обстоятелството, че към настоящия момент /след значително по-дълъг срок от 6 месеца/ оспореният акт все още не е влязъл в сила, а няко от предписанията междувременно са изпълнени от администатоа НАП.

С оглед изхода на спора, основателно се явява искането за присъждане на направените по делото разноски и от двете насрещни страни, съответно на основателната част на жалбата за жалбоподателя НАП, а за ответника КЗЛД-съответно на неоснователната част на жалбата, при съобразяване с размера , установен вчл. 24 от Наредба за заплащането на правната помощ, вр. чл. 37 от Закона за правната помощ за защитата им осъществена от

юрисконсулти. Предвид голямата фактическа сложност на делото, процесуалната активност на пълномощниците - юрисконсулти, обема и качеството на осъществената процесуална дейност, съдът прие, че юрисконсултското възнаграждение следва да се определи в максималния размер от 240 лева. На ответника се присъждат 194 лв., съответно на неоснователната част на жалбата а на жалбоподатеиля- 46 лв., съответно на основателната част от жалбата. От заплатеното от жалбоподателя възнаграждение за вещи лица общо в размер на 2 800 лв., върху ответника следва да се възложи сумата в размер на 533 лв., съотв. на основателната част от жалбата, като същият се осъди да заплати на жалбоподателя разноски общо в размер на 579 лева.

Воден от гореизложеното, Административен съд София-град, Второ отделение, 23-ми състав

Р Е Ш И:

ОТМЕНЯ по жалба на Националната агенция за приходите, ЕИК[ЕИК], Решение № ППН-02-399 от 22.08.2019 г., издадено от Председателя на Комисията за защита личните данни , В ЧАСТТА МУ относно Разпореждания № 7, 14, 15 изцяло, Разпореждане № 5 в частта му: "Да се предприемат небходимите действия за създаването на одитни записи на отделните събития и дневници /журнали/ за привилегированите потребители" и Разпореждане №16 в частта му относно "повторното използване на такива данни".

ОТХВЪРЛЯ жалбата в ОСТАНАЛАТА Й ЧАСТ.

ОСЪЖДА Националната агенция за приходите с ЕИК[ЕИК] да заплати на Комисията за защита личните данни сумата в размер на 194 /сто деветдесет и четири/ лева, разноски по делото.

ОСЪЖДА Комисията за защита личните данни да заплати на Националната агенция, ЕИК[ЕИК] за приходите разноски в размер на 579 / петстотин седем десет и девет/ лева.

Решението подлежи на обжалване с касационна жалба в 14-дневен срок съобщаването му.

Решението да се съобщи на страните чрез изпращане на преписи от него.

СЪДИЯ: