Р Е Ш Е Н И Е
№ 3088

гр. София, 30.01.2025 г.

В ИМЕТО НА НАРОДА

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 30 състав,** в публично заседание на 30.10.2024 г. в следния състав:

СЪДИЯ: Мая Сукнарова

при участието на секретаря Кристина Алексиева, като разгледа дело номер **1558** по описа за **2024** година докладвано от съдията, и за да се произнесе взе предвид следното:

Производството е по реда на чл.145 и сл. от Административнопроцесуалния кодекс (АПК) във вр. с чл.38, ал.7 във вр. с ал.3 от Закона за защита на личните данни (ЗЗЛД).

Образувано е по жалба от Националната агенция за приходите (НАП) срещу решение № ППН-02-399 от 22.08.2019 г., издадено от Комисията за защита личните данни (КЗЛД), с което на основание чл.58, §2, б.„г“ във вр. с чл.57, §1, б.„а“ и чл.83, §2, б.„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 - Регламент (ЕС) 2016/679) на НАП е разпоредено като администратор на лични данни да съобрази операциите по обработването на данни, като:

1. 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 на 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. Предприеме подходящи технически и организационни мерки с цел повишаване защитата при обработка на лични данни в приложения за електронни услуги към

гражданите.
3. Изготви в пълен обем правила и процедури за защита на личните данни, като за всяка една от подържаните в НАП информационни системи се разработят правила за обработка на личните данни в тях.
4. Предвиди в политиките за формиране на профилите за достъп до приложенията (Privacy By Design), 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. Предприеме 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 Management, PAM) и Система за управление и анализ на събитията, отразени в дневниците (Security information and event management, SIEM).
6. 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. Извърши анализ на риска на системите и операциите по обработването, включващи изготвени правила и функционални задължения за работа на всяка информационна система.
8. 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 по чл.35, §4 от Регламент (ЕС) 2016/679.
9. Изготви правила и процедури за оценка на въздействието при защита на данните при първоначално стартиране на нови информационни системи и приложения.
10. 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 (Privacy By Design, Privacy By Redesign и Privacy By Default).
11. Обнови операционните системи от Windows 2008R2 към актуални версии от 2013 г. и 2016 г., и на СУБД Oracle 11.2.0.2 към актуална версия Oracle 12, за да не се създава потенциална опасност за сигурността на данните след 2020 г., преди изтичане на срока за тяхната поддръжка.
12. Изгради център за възстановяване работоспособността на системите в реално време (Disaster Recovery Center).
13. Изготви политики за обработване на специални категории данни, съгласно чл.9 от Регламент (ЕС) 2016/679.
14. Изготви политики за повторно използване на личните данни на субектите.
15. Изготви политики и вътрешни правила за анонимизиране, архивиране и унищожаване на електронните данни, използвани еднократно.
16. 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. Изготви стратегия и политики за криптиране на данни от архивни или еднократно извършвани справки.
18. 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.Актуализира длъжностните характеристики на служителите на НАП с включени клаузи, касаещи обработването на лични данни.
20. Изготви вътрешни правила за обучение и тренировка на служителите на НАП за действия в случаи на незаконосъобразно обработване на лични данни.
С жалбата се твърди, че оспореният акт е издаден при съществени нарушения на административнопроизводствените правила и в противоречие с материалния закон. Дадените разпореждания били общо формулирани и непълно дефинирани, което създавало неясноти и препятствало тяхното изпълнение. Даденият 6-месечен срок за изпълнение на разпорежданията бил прекалено кратък. Разпорежданията на КЗЛД, отнасящи се до изготвяне на процедури, правила и политики били обосновани от неправилни констатации и изводи на проверяващия екип, както и необвързани от действащ нормативен или друг задължителен за приложение акт.
Ответникът – Комисията за защита на личните данни оспорва жалбата като неоснователна и моли същата да бъде отхвърлена. Претендира присъждане на юрисконсултско възнаграждение.
По жалбата е постановено решение № 565/02.02.2023 г. по адм. дело № 10477/2019 г. по описа на Административен съд – София град. С него са отменени изцяло разпореждания № 7, 14 и 15, разпореждане № 5 е отменено в частта му „Да се предприемат необходимите действия за създаване на одитни записи на отделните събития и дневници (журнали) за привилегированите потребители”, а разпореждане № 16 е отменено в частта му относно повторното използване на лични данни на деца. Жалбата в останалата й част е отхвърлена. Решението е обжалвано само в отхвърлителната му част. С решение № 1398/07.02.2024 г. по образуваното пред него адм. дело № 3781/2023 г. Върховният административен съд го е отменил и е върнал делото за ново разглеждане в частта, с която жалбата е отхвърлена като са дадени задължителни указания по тълкуването и прилагането на закона.
При новото разглеждане на делото, настоящият състав на Административен съд – София град, установи следната фактическа обстановка:
Националната агенция за приходите е администратор на лични данни по смисъла на чл.4, т.7 от Общия регламент относно защитата на личните данни.
Административното производство пред КЗЛД е започнало по изпратено от НАП Уведомление с 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.
На 18.07.2019 г. пред КЗЛД е представена докладна записка за извършен анализ на постъпилото Уведомление с вх. № ППН-02-399#1/18.07.2019 г.
На проведено на 19.07.2019 г. заседание КЗЛД се е самосезирала 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 НАП. Прието е решение за извършване на проверка.
Със заповед № РД-15-249/19.07.2019 г. на председателя на КЗЛД е определен проверяващ екип. На НАП е изпратено уведомление за проверката. Същата е започнала на 22.07.2019 г. в административната сграда на ЦУ на НАП в [населено

място]. Във връзка с това са изпратени два въпросника, касаещи 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 е предоставила изисканите отговори.
Съставени са Констативни протоколи (КП) от 02.08.2019 г. и от 08.08.2019 г., от които се установява, че са проведени работни срещи с определените от НАП длъжностни лица за оказване на съдействие на проверяващия екип.
На 14.08.2019 г. е бил съставен приемо-предавателен протокол по искане за предоставяне на информация за списъка и броя на починали лица, заповед № З-ЦУ-745/25.05.2018 г. и заповед № З-ЦУ-744 от 22.05.2019 г., както и утвърден регистър на категориите дейности по обработване.
На същата дата (14.08.2019 г.) е 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.
На 20.08.2019 г. е съставен Констативен акт (КА) с вх. № ППН-02-462, който е послужил като основание за издаването на оспореното решение № ППН-02-399 от 22.08.2019 г. В КА е записано, че 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 са: - общ брой на всички физическите лица, който включва български и чужди граждани, в това число с прекратена регистрация - 6 074 140 бр.; - общ брой на всички активни физически лица, който 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 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.; - 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 на 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 които е осъществен неоторизиран достъп – 427 GB; - сървърът до който е осъществен нерегламентираният достъп работи с остаряла версия на операционната система Windows 2008R2 и по-стара версия на СУБД Oracle 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.

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., е посочено, че при извършената проверка 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; - 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;- 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. VAT 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 със съответните RO, електронен адрес, длъжност, пароли; - данни, свързани с информационни системи MOSS / VoES: - BIC, IBAN, 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 MOSS - 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, Агенция по заетостта, Агенция за социално подпомагане, Националната здравноосигурителна каса и др.

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 - ОИСР: - 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 ОИСР (CRS); - данни от специална схема за облагане с ДДС – съкратено обслужване на едно гише (информационни системи MOSS и VOES); - данни от програмен продукт EUROFISC - борба с данъчните измами на европейско ниво; - информация, обменяна, обработвана и съхранявана в информационни системи, разработени съгласно изискванията 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; 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; - 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 §19к от ПЗР на ЗЗО; - списък с 1 064 млн. идентификатора и данни за заплата, данъци, осигуровки; -регистрационни данни на физически и юридически лица; - лични данни за служители на НАП към 2009 г.; лични данни за физически лица от ГД „ГРАО”; 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.

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 с рег. № 93-00-1383 от 22.03.2019 г.

Изводите на КЗЛД, с които са аргументирани дадените предписания са следните:

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.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;

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 техния вид и чувствителност (съобразно оценката на риска);

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 (Privacy By Design), 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;
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 Management, 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 (Security 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;
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;
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;
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, §4 от Регламент (ЕС) 2016/679;
9. Липсват документирани правила и процедури за оценка на въздействието при защита на данните при първоначално стартиране на нови информационни системи и приложения;
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 (Privacy By Design, Privacy By Redesign и Privacy By Default);
11. Не са предприети действия за обновяване на операционните системи

от Windows 2008R2 към актуални версии от 2013 г. и 2016 г., и на СУБД Oracle 11.2.0.2 към актуална версия Oracle 12, което създава потенциална опасност за сигурността на данните след 2020 г., когато изтича срокът за тяхната поддръжка;
12. Няма изграден център за възстановяване работоспособността на системите в реално време (Disaster Recovery Center);
13. Липсват политики за обработване на специални категории данни съгласно чл.9 от Регламент (ЕС) 2016/679;
14. Липсват политики за повторно използване на личните данни на субектите;
15. Липсват политики и вътрешни правила за анонимизиране, архивиране и унищожаване на електронните данните, използвани еднократно (различни видове справки и заявки);
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;
17. Липсват приети стратегия и политики за криптиране на данни от архивни или еднократни извършвани справки;
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;
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;
20. Липсват вътрешни правила за обучение и тренировка на служителите на НАП за действия в случаи на незаконосъобразно обработване на лични данни.
Издадено е оспореното решение № ППН-02-399 от 22.08.2019 г. на КЗЛД, от което предмет на разглеждане в настоящото съдебно производство са разпореждания № 1, 2, 3, 4, 5 в частта му „да внедри Система за управление на привилегиите на потребителите (Privileged Access Management, PAM) и Система за управление и анализ на събитията,

отразени в дневниците (Security information and event management, SIEM)", 6, 8, 9, 10, 11, 12, 13, 16 в частта му „да изготви политики и процедури за обработка на лични данни на деца, проследяващи механизми и Cookies (бисквитки), определяне срока за съхранение и задържане на данните", 17, 18, 19 и 20.

При тези данни и след като извърши дължимата на основание чл.168, ал.1 от АПК проверка на всички основания по чл.146 от АПК съдът намира следното:

Оспореното решение е издадено от компетентен орган. Съгласно чл.6, ал.1 от ЗЗЛД, КЗЛД е независим държавен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на този закон и на Регламент (ЕС) 2016/679. Тази своя функция Комисията осъществява, упражнявайки предоставените й с чл.10, ал.1 от ЗЗЛД правомощия.

Обжалваното решение е прието при наличие на необходимия кворум и с изискуемото мнозинство (чл.9, ал.3 от ЗЗЛД). Съгласно чл.7, ал.1 от ЗЗЛД, Комисията е колегиален орган и се състои от председател и 4 членове, а решенията се вземат с мнозинство от общия брой на членовете (чл.9, ал.3). Същото следва да бъде подписано от всички членове, участвали в гласуването. В случая за оспореното решение са гласували четирима „за" и нито един против, поради което безспорно е формирано мнозинство и решението е валидно взето.

Доколкото приложимият специален закон ЗЗЛД не съдържа специални изисквания към формата и съдържанието на акта, същият следва да отговаря на изискванията за форма, предвидени в чл.59 от АПК, като съдът намира, че законоустановената форма е спазена - актът съдържа дължимите по чл.59, ал.2 от АПК реквизити, в това число и фактическите и правни основания за издаването му.

В производството не са допуснати съществени нарушения на административнопроизводствените правила, които да съставляват самостоятелно основание за неговата отмяна. Производството е започнало по изпратено от НАП Уведомление вх. № ППН-02-399/17.07.2019 г. по чл.33 от Регламент (ЕС) 2016/679, въз основа на което КЗЛД се е самосезирала и след обсъждане на КА с рег. № ППН-02-462/20.08.2019 г. е взето процесното решение.

По приложението на материалния закон съдът намира следното:

Преди всичко следва да се посочи, че разпоредбите на чл.59, ал.1 от ЗЗЛД и чл.24, §1 от Регламент (ЕС) 2016/679 задължават администратора на лични данни не само да прилага подходящи технически и

организационни мерки при обработването на лични данни, но и да е в състояние да докаже, че това обработване се извършва в съответствие със закона. Това означава, че доказателствената тежест да докаже, че законосъобразно е обработвал личните данни, се възлага на администратора на лични данни. Тоест разпоредбите на чл.59, ал.1 от ЗЗЛД и чл.24 от Регламент (ЕС) 2016/679 създават оборима презумпция за незаконосъобразното обработване на личните данни, ако администраторът не докаже, че обработването им е в съответствие със закона. При това посоченото съответствие следва да е било налице към момента на постановяване на оспорения административен акт, тъй като законосъобразността на административния акт се разглежда към момента на неговото издаване. Това означава, че при проверката за законосъобразност следва да се вземат предвид обстоятелствата и правните норми, валидни в момента, в който актът е бил издаден.

В тази връзка следва да се приемат за неоснователни възраженията на жалбоподателя, направени с представени пред настоящата съдебна инстанция писмени бележки, които възражения в основната си част се свеждат до това, че по-голямата част от дадените с оспореното решение на КЗЛД предписания са вече изпълнени. Установяването на наличието, респ. липсата на технически и организационни мерки, гарантиращи, че обработването на личните данни се извършва в съответствие със закона, е към момента на постановяване на акта. В случая, въпреки че в хода на производството се установи, че част от мерките действително са били изпълнени, ответникът не признава това изпълнение. Наличието на такова би било предмет на последваща проверка, каквато все още не е направена. И поради тази причина законосъобразността на дадените разпореждания следва да се разгледа към момента на издаване на обжалваното решение.

По отношение на възражението за даден кратък срок за изпълнение на посочените в оспореното решение мерки, съдът намира, че въпросът дали срокът е бил достатъчен за изпълнение на оспорените предписания е предмет също на последваща проверка по изпълнение на тези предписания.

Освен това, при новото разглеждане на делото настоящият съдебен състав следва да съобрази дадените с решение № 1398/07.02.2024 г. на Върховния административен съд по образуваното пред него адм. дело № 3781/2023 г. указания, като при решаването на спора игнорира заключението по третата приета при предходното разглеждане на делото експертиза без да основава правните си изводи върху него.

1.Съдът разглежда заедно Разпореждане № 3 и Разпореждане № 13 от решение № ППН-02-399 от 22.08.2019 г., издадено от Комисията за

защита личните данни, тъй като и двете се отнасят до обработване на специална категория лични данни.
С разпореждане № 3 на НАП е указано да изготви в пълен обем правила и процедури за защита на личните данни, като за всяка една от подържаните в НАП информационни системи се разработят правила за обработка на личните данни в тях.
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, §1, б.„е“ от Регламент (ЕС) 2016/679. В чл.66, ал.2 от ЗЗЛД законодателят е посочил мерки, които администраторът е длъжен да предприеме за защита на обработваните данни за постигане на конкретно посочени цели. Според чл.4, § 12 от Регламента, „нарушение на сигурността на лични данни" е 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.
Проверката, въз основа на която са констатирани съответните нарушения от страна на НАП и във връзка, с които са дадени оспорените разпореждания е започнала по повод осъществен на 15.07.2019 г. неоторизиран достъп до обработваните от НАП бази данни с лични данни (име, ЕГН), като част от съдържаща се в тях информация е публикувана в интернет пространството.
В изслушаната по делото първа съдебно-техническа експертиза (СТЕ), вещото лице се позовава на наличните в НАП документи, съдържащи информация относно начина на обработване на лични данни, сред които: Указанията за обозначаване и работа с информационна версия 3.1 от 2018 г., „Политика по информационна сигурност на НАП“, версия 3, от май 2016 година, както и заповед № ЗЦУ-746/25.05.2018 г., с която се утвърждава политика за защита на личните данни и заповед № ЗЦУ–585/24.03.2021 г. По отношение на първите три документа вещото лице е констатирало, че същите съдържат кратки указания, основни определения и тълкувания на понятията, свързани със защита на лични данни, без да съдържат конкретни правила за обработка на личните данни в отделните поддържани в НАП информационни системи. Установено е, че в различни периоди НАП е създала много документи с различни инструкции и правила, касаещи личните данни, но те не били обединени и структурирани в единна политика или единен йерархичен документ.

Това създавало проблеми при ползването. Експертът е посочил, че е запознат с Инструкция № 2, която касаела различни дейности в НАП, но тя не съдържала детайлни указания за всички дейности, които са необходими във връзка със сигурността на данните.
Според вещото лице, издадената на 24.03.2021 г. заповед № ЗЦУ–585 на изпълнителния директор на НАП съдържала утвърдени роли за достъп до информационните системи на НАП, където се обработвали и визуализирали различен по обхват данни и се създавали коректни правила за защита на различните категории лични данни.
Съдът обаче намира, че доколкото тази заповед, е издадена след датата на издаване на оспореното решение, същата не следва да се коментира при преценката за законосъобразност на оспорения акт.
От заключението по втората СТЕ се установява, че към 15.07.2019 г. НАП е разполагала с няколко документа, в които са заложени основни правила и общи кратки указания и тълкувания, свързани със защитата на лични данни. В тези документи не били регламентирани конкретни правила за събиране, обработване и съхранение на лични данни в и чрез притежаваните и използваните информационни системи от НАП. Предприетият от НАП модел за осигуряване на защита на лични данни чрез общи правила се осъществявал чрез внедрена Система за управление на сигурността на информацията (СУСИ), базирана на международно признатия стандарт за сигурност на информацията БДС ISO/IEC 27001/2014. Правилата и изкисванията в този стандарт били по-разширени от изискванията, заложени в Регламент (ЕС) 2016/679 и следвало да се приемат за достатъчни при осигуряване на защитата на личните данни.
С оглед на тези констатации съдът приема, че произходащите от НАП документи, свързани с обработката и съхраняването на лични данни към датата на установяване на изтичането на информация, доколкото съдържат само основни правила и общи кратки указания, свързани със защитата на личните данни, не регламентират конкретни правила за събиране, обработване и съхранение на лични данни в и чрез притежаваните и използваните информационни системи от НАП, поради което даденото разпореждане № 3 се явява законосъобразно.
С разпореждане № 13 на НАП е указано да изготви политики за обработване на специални категории данни, съгласно чл.9 от Регламент (ЕС) 2016/679.
Съгласно чл.51, ал.1 от ЗЗЛД, 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. Съгласно чл.9, § 1 от Регламента, 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. Според определението, дадено в т.15 на чл.4 от Регламента „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.

Нормата на чл.9, §2, б.„б“ от Регламента гласи, че параграф 1 не се прилага, ако 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, съгласно което: „Специални категории лични данни, които се нуждаят от по-голяма защита, могат да бъдат обработвани единствено за здравни цели, когато е необходимо тези цели да бъдат постигнати в полза на отделни физически лица и на обществото като цяло, по-специално в рамките на управлението на услугите и системите за здравеопазване или социални грижи, включително обработването от страна на органите за управление и от централните национални здравни органи на такива данни за целите на контрола на качеството, информацията за управлението и общото наблюдение на национално и местно равнище на системата за здравеопазване или социални услуги, както и за осигуряване на непрекъснатост на здравното обслужване или на социалните услуги и на трансграничното здравно обслужване или за целите на сигурността, наблюдението и предупрежденията в сферата на здравеопазването, или за

целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели въз основа на правото на Съюза или националното право, което трябва да отговаря на цел от обществен интерес, както и за проучванията в областта на общественото здраве, провеждани в обществен интерес. Поради това настоящият регламент следва да предвижда хармонизирани условия за обработването на специални категории лични данни за здравословното състояние по отношение на специфични нужди, по-специално когато обработването на тези данни се извършва за определени цели, свързани със здравето, от лица, обвързани от правното задължение за професионална тайна. Правото на Съюза или националното право следва да предвижда конкретни и подходящи мерки за защита на основните права и личните данни на физическите лица. Държавите членки следва да разполагат с възможност да запазят или да въведат допълнителни условия, включително ограничения, по отношение на обработването на генетични, биометрични или данни за здравословното състояние. Това обаче не следва да възпрепятства свободното движение на лични данни в рамките на Съюза, когато тези условия се прилагат за трансгранично обработване на такива данни.” Тоест предвидена е дерогация от забраната за обработване на специални категории лични данни, 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.

Съгласно съображение 35 от Регламент (ЕС) 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. Това 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."
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 или НЕЛК. Не е необходимо да се вписва и номер на решение. В същото време обаче в НАП постъпват решения на експертни лекарски комисии, съдържащи данни за % на намалена 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 страна 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 от

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, §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.

По изложените съображения настоящият съдебен състав приема, че НАП обработва специални категории лични данни съгласно чл.9 от Регламент 2016/679 за цели извън случаите по чл.9, §2, б.„б“ за установяване на данъчни и осигурителни задължения, предвид което са приложими и се прилагат политиките и процедурите, свързани с обработването на данъчна и осигурителна информация в НАП и е необходимо Агенцията 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. 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 номерът на решението към датата на издаване на оспореното решение на КЗЛД. 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 представлявят данни за здравословното състояние на лицето по чл.4, т.15 от Регламента.

Решенията на експертни лекарски комисии, съдържащи данни за % на намелена работоспособност също следва да се характеризират по описания начин и попадат в приложното поле на съображение 35 и 54 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. Член 9, §1 от Регламента установява изрична забрана за обработване на такъв тип данни. В чл.9, §2 от Регламента са установени изчерпателно изброени изключения от този принцип. В съответствие с чл.9, §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, §2, б.„б“ от Регламента. Целта на чл.9, §2, б.„б“ от Регламента е именно да могат да се събират специални лични данни в изчерпателно определени хипотези. Неслучайно 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 изложеното необосновано се явява твърдението на жалбоподателя, че „здравословното състояние“ не попада 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 чл.8, §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 чл.9, §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, §1 от Регламента, НАП е длъжна да

подхожда с необходимите завишени изисквания към нея, защото тя попада в специалната категория лични данни (чувствителни данни).
В същото време по делото не се установи събиране, обработване и съхранение на чувствителни лични данни или други специални категории лични данни, съгласно чл.9 от Регламент 2016/679, като религия, пол, интереси, расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и генетични данни или биометрични данни.
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. 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 съдът определя 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 разпореждане № 1, НАП следва 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 на 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.
Според разпореждане № 4, НАП следва да предвиди в политиките за формиране на профилите за достъп до приложенията (Privacy By Design), 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.
Според първата приета по делото СТЕ, към момента на изготвяне на експертизата вече са били взети мерки за въвеждане в активната директория на правила за достъп на отделните групи потребители и привилегированите потребители имали ограничен специализиран достъп до информационните ресурси. Всеки привилегирован потребител имал

достъп до определени информационни ресурси, а не до целия информационен ресурс. Този специализиран достъп бил ограничен до степен, даваща възможност за изпълнение на служебните задължения на служителите по длъжностна характеристика. Конкретните задължения на привилегированите потребители били определени със заповед на изпълнителния директор на НАП, а именно заповед № ЗЦУ – 585/24.03.2021 г., с утвърдени роли за достъп до информационните системи на НАП, където се обработвали и визуализирали различни по обхват данни и се създавали конкретни правила за защита на различните категории лични данни.

Съдът приема, че тъй като е издадена след постановяване на оспореното решение на КЗЛД, тази заповед не следва да се взема предвид при преценката за законосъобразност на акта.

Според втората СТЕ, активната директория била въведена за всички служители на НАП към 19.07.2019 г., чрез което се осъществявал контрол на достъпа и се делегирали 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 изготвяне на експертизата. Тази заповед регламентирала утвърдените роли за достъп до Информационни системи на НАП, визуализиращи и обработващи различен по обхват данни. Същата заповед била предхождана от редица други, отменени от нея, като непосредствено предхождаща тази от 19.07.2019 г. била заповед № 9/ЗЦУ–472/01.04.2019 г. Според вещото лице се касаело до софтуерен механизъм, чрез който се раздават права за достъп на отделните потребители. След внедряване на приложението, разработчиците трябвало да имат само сервизен достъп, но към момента на извършване на експертизата не можело да се каже със сигурност дали това е било така и към 15.07.2019 г.

И според двете СТЕ, към момента на извършване на експертизите имало въведена активна директория за правила на достъп на отделните групи потребители и привилегированите потребители имали ограничен специализиран достъп до информационните ресурси. Следва да се посочи обаче, че в първата експертиза, вещото лице не може да твърди със сигурност дали такава активна директория е била създадена към момента на изтичането на данни на 15.07.2019 г.

Втората СТЕ препраща към заповед от 01.04.2019 г., въз основа на която съдът констатира единствено, 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 е имал достъп до определени информационни ресурси, а не до целия

информационен ресурс, както и дали активната директория е работела 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 Регламента, 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.
3. Разпореждане № 5 от оспореното решение към НАП съдържа следното изискване: Да предприеме необходимите действия за създаване на одитни записи на отделните събития и дневници (журнали) за привилегированите потребители. С решение № 565/02.02.2023 г. по адм. дело № 10477/2019 г. тази част от разпореждането е отменена. Решението в тази му част не е обжалвано, съответно е влязло в сила и не е предмет на обсъждане от настоящия съдебен състав. Съдът следва да се произнесе единствено по частта от разпореждането, с която от НАП е изискано да внедри Система за управление на привилегиите на потребителите (Privileged Access Management, PAM) и Система за управление и анализ на събитията, отразени в дневниците (Security information and event management, SIEM).
Съгласно първата СТЕ, НАП е разполагала със Система за управление на привилегиите на потребителите (Privileged Access Management, PAM), която към 15.07.2019 г. е функционирала в тестова среда, а в момента на изготвяне на експертизата вече е била напълно внедрена. Към 15.07.2019 г. Агенцията разполагала със система за одитиране и анализ на информационната инфраструктура (QualysGuard), доставена през 2015 г. В резултат на извършена оценка през 2019 г. на стратегическите рискове в НАП била идентифицирана необходимост от придобиване на Security information and event management и били планирани средства за такава система. Към датата на посещението на вещото лице в НАП, няколко софтуера, които в цялост изграждат такава система били в процес на пускане в експлоатация. Според вещото лице, изготвило първата експертиза, при посещението му в НАП в началото на 2020 г. били в процес на инсталиране 3 софтуера, но нямало данни, кога са придобити от НАП. Експертът подчертава, че в НАП процесът по придобиване и инсталиране бил доста дълъг, защото първо се инсталирали в тестова среда, правели се обучения на администратори и чак впоследствие се инсталирали в работна среда. Обяснява още, че е изследвал системата за контрол на потребителите, включително и привилегированите потребители, в която също имало данни от 15.07.2019 г., но тогава системата работела с непълен капацитет, тъй като все още била тестова.

Съгласно втората СТЕ към 15.07.2019 г. НАП разполагала със система за управление привилегиите на потребителите (Privileged Access Management), работеща в тестова среда и в процес на внедряване, а към момента на изготвяне на експертизата същата била напълно функционална. През 2015 г. била 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 разполагала с посочените системи, а непосредствено след инцидента по изтичане на данни 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, Identity and Access Management – софтуер за управление на идентичността и достъпа.

И според двете СТЕ към момента на проверката Система за управление на привилегиите на потребителите (Privileged Access Management, PAM) и Система за управление и анализ на събитията, отразени в дневниците (Security information and event management, SIEM) били в процес по внедряване, но не са били функционали.

При тези данни, съдът приема, че обсъжданото разпореждане № 5 в частта му „да внедри Система за управление на привилегиите на потребителите (Privileged Access Management, PAM) и Система за управление и анализ на събитията, отразени в дневниците (Security information and event management, SIEM)" към момента на издаването му е било законосъобразно.

4. Разпореждане № 6, 8, 9, 10 се разглеждат в съвкупност, тъй като се отнасят до оценка и управление на риска, както и до въвеждане на нови системи.

Съгласно разпореждане № 6, НАП трябва да 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.

Според разпореждане № 8, НАП следва да 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 по чл.35, §4 от Регламент (ЕС) 2016/679.

Разпореждане № 9 въвежда задължение НАП да изготви правила и процедури за оценка на въздействието при защита на данните при първоначално стартиране на нови информационни системи и

приложения.
А с разпореждане №10 се посочва, че НАП трябва да 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 (Privacy By Design, Privacy By Redesign и Privacy By Default).
Съгласно чл.35, §1 от Регламент (ЕС) 2016/679, 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. Според чл.35, §3, б.„б“ от Регламента, оценката на въздействието върху защитата на данните, посочена в параграф 1, се изисква по-специално, в случай на 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, §4 от Регламента постановява, че надзорният орган съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно параграф 1. Надзорният 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.

Съгласно чл.25, §1 от Регламента, 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.

Тук следва да се има предвид приетото от съда в мотивите, отнасящи се до 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, §3, б.„б“ е приложим в настоящия случай, с оглед обработването на данни по чл.9 от Регламента от страна на НАП. 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, следва 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. Аргументът на НАП, че „след влизане в сила на Регламент (ЕС) 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.

В случая, от заключението по първата изслушана по делото 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 изготвяни отделни правила за всяка система, а анализ на 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 се извършвали съгласно утвърдени в НАП процедура и Методика за оценка на риска за информационната сигурност и посочени следните допълнителни мерки: Подписани били декларации от всички служители по чл.14, ал.3 от ЗНАП и чл.61, ал.1 от 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), като в тях били включени специални изисквания. Към момента на разработването на информационните системи (ИС) в НАП изискванията на Регламент (ЕС) 2016/679 за оценка на въздействие (риска) не били действащи, поради влизането му в сила през месец май 2018 г. Служителите на НАП посочили, че след влизане в сила на Регламент (ЕС) 2016/679 в НАП не били 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 на 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 извършвала оценка на риска, като се анализирали заплахите за информационната система заедно с потенциалните уязвимости и съществуващи мерки. По отношение на принципа „Privacy By Design“, по време на срещите било посочено, че тълкуването на НАП било, 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, следвало 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.

От заключението по 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 (ЕС) 2016/679 тези правила били съпоставими и следвало да се приеме, че отговарят общо на изискванията. Тези правила били приложими за всяка една информационна система, притежавана и използвана от НАП от момента на нейното първоначално въвеждане в експлоатация. В периода м. януари – м. април 2018 г. 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 (ЕС) 2016/679, като в част от системите и начините за предаване на данни към системите на други институции, там където било възможно, били взети мерки за анонимизиране и минимизиране на данните.

В писмените си бележки от 21.02.2024 г., представени от жалбоподателя в настоящото съдебно производство се твърди, че със заповед № З-ЦУ-1830/17.10.2022 г. на изпълнителния директор на НАП е утвърдена Методология за оценка на риска за субектите на данни с приложения № 1, 2 и 3, касаещи обработката на данните, изчисляване на пряката идентификация на субектите на данни и изчисление на точките при обстоятелствата на нарушението, както и пълен пакет от вътрешни административни документи в областта на законосъобразното обработване и защита на личните данни. Методологията била неразривно свързана с разработени Вътрешни правила за изготвяне на оценка на въздействието върху защитата на личните данни, утвърдени със заповед № З-ЦУ-1830/17.10.2022 г.

Съдът приема, че тъй като заповед № З-ЦУ-1830/17.10.2022 г. е издадена след постановяване на оспореното решение на КЗЛД, същата не следва да се взема предвид при преценката за законосъобразност на акта. Същото се отнася и до предприетите от НАП мерки по изпълнение на разпореждания № 8 и 10, които също са предприети след издаване на оспореното решение.

При тези обективни данни по делото съдът приема, че разпорежданията свързани с предписания № 6, 8, 9 и 10 са законосъобразни.

5. Според разпореждане № 11, НАП трябва да обнови операционните системи от Windows 2008R2 към актуални версии от 2013 г. и 2016 г., и на СУБД Oracle 11.2.0.2 към актуална версия Oracle 12, за да не се създава потенциална опасност за сигурността на данните след 2020 г., преди изтичане на срока за тяхната поддръжка.

Съгласно първата експертиза, към момента на изготвянето й операционните системи от Windows 2008R2 са модернизирани към актуална версия от 2013г. и 2016 г., както и на СУБД Oracle 11.2.0.2 към актуална версия Oracle 12. Не 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 Windows и на СУБД Oracle 11.2.0.2, необходимо било време да се модифицират, а също и допълнително при внедряване на всяка по-нова версия, трябвало да се извършва тестване и анализ, с цел установяване работоспособност и непрекъсваемост на системите. До същата констатация стига и вещото лице по втората СТЕ.

С жалбата не е оспорено, че към момента на издаване на решението на КЗЛД е прилагана по-стара версия на Windows 2008R2 и на СУБД Oracle, а оплакването касае само срока, предвиден за въвеждането на новите системи (тяхното обновяване). Видно и от двете СТЕ, НАП е в процес по обновяване на системите, но това е бавен процес с оглед осигуряването функционирането на приложните системи.

С писмените бележки, представени пред настоящата съдебна инстанция жалбоподателят твърди, че с цел елиминиране на потенциални опасности за сигурността на данните, в случай на идентифициране в хода на изпълнение на процес „Администриране на информационни системи, друг системен софтуер и управление на хардуерните устройства" от Дирекция ИСЕУ своевременно се предприемат действия за обновяване при необходимост на операционни системи от Windows към по-висока версия, както и на БД Oracle по отношение на съответствие ИС на НАП, работещи с остаряла версия на операционната система за обновяването им още преди изтичане на тяхната поддръжка. Във всички функционални спецификации за поддръжка на ИС се засягали нефункционални изисквания към технологичната среда на НАП, с която следвало да са съвместими новоразработваните или надградени ИС и ЕУ на НАП. Отбелязано е, че операционните системи от Windows СУБД Oracle 11.2.0.2 са обновени към актуални версии от 2021 и 2022 г.

С това съдът приема, че разпореждането към момента на издаването си е било законосъобразно като към настоящия момент администраторът на лични данни все още работи по изпълнението му.

6. Според разпореждане № 12, НАП следва да изгради център за възстановяване работоспособността на системите в реално време (Disaster Recovery Center).

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 (Disaster Recovery Center), 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 Disaster Recovery Center 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.
С жалбата си до съда НАП не е оспорил констатираната липса на център за възстановяване работоспособността на системите в реално време към момента на издаване на оспореното предписание, а предоставения за това срок от 6 месеца.
С оглед на изложеното съдът приема, че към датата на постановяване на разпореждане № 12 същото е било законосъобразно.
Следва да се отчете, че в писмените си бележки пред настоящия съд жалбоподателят посочва, че за осигуряване на непрекъснатост на най-критичните бизнес процеси, НАП поддържа и резервен изчислителен център, разположен на достатъчно отдалечено разстояние от основния. В Центъра за бедствия и аварии на ЦУ на НАП се резервирали и архивирали данни от критичните за НАП информационни системи. Центърът бил изграден с цел превенция на риска от загуба на данни и осигуряване на работоспособност и непрекъсваемост на ИС. Дали обаче НАП е изпълнила предписанието за изграждането на център за възстановяване работоспособността на системите в реално време е предмет на установяване чрез съответната проверка.
7. Разпореждания № 16 и 17 се разглеждат заедно, тъй като се отнасят до обработката на данни и съхранението на архиви.
Според разпореждане № 16, НАП трябва 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.
С решение № 565/02.02.2023 г. по адм. дело № 10477/2019 г. е отменена частта от разпореждането относно повторното използване на личните данни на деца. Решението в тази част не е обжалвано, съответно е влязло

в сила и не е предмет на обсъждане от съда. Съдът следва да се произнесе единствено по частта, с която от НАП е изискано да изготви политики и процедури за обработка на лични данни на деца, проследяващи механизми и Cookies (бисквитки), определяне срока за съхранение и задържане на данните.
Съгласно съображение 38 от Регламент (ЕС) 2016/679, 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. Според чл.57, §1, б.„б“, 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.
С жалбата не е била оспорена констатираната липса на правила и процедури при обработване на лични данни на деца. В писмените бележки на жалбоподателя, представени пред настоящата съдебна инстанция на 21.02.2024 г. е посочено, че със заповед № З-ЦУ-1830/17.10.2022 г. на изпълнителния директор на НАП са утвърдени Политики за обработване на лични данни на деца в НАП и Политика за поверителност при използване на интернет страницата на НАП, като в последната подробно били изяснени въпросите, свързани с Cookies (бисквитки), видовете „бисквитки”, сроковете за съхранение на данните, използвани функционалности за защита на портала за ЕУ на НАП и др. И двата документа били публикувани на официалната интернет страница на НАП и били общодостъпни за физически лица – клиенти на Агенцията.
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 (ЕС) 2016/679, и приема, че това разпореждане е законосъобразно.
Доколкото към момента на издаване на това разпореждане правила относно обработването на лични данни на деца не са били приемани, а нова проверка за изпълнение на разпореждане № 16 към настоящия момент не е осъществена, съдът намира, че посоченото разпореждане към

момента на издаването си е било законосъобразно.
Относно разпореждане № 17, с което от НАП е изискано да изготви стратегия и политики за криптиране на данни от архивни или еднократни извършвани справки, следва да се посочи, че с жалбата не е оспорена констатираната липса 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, §1, б.„а“ от Регламента гласи, че като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, inter alia, когато е целесъобразно псевдонимизация и криптиране на личните данни.
В писмените си бележки от 21.02.2024 г. жалбоподателят твърди, че 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 Инструкцията за мерките и средствата за защита на лични данни, обработвани в НАП и реда за движение на преписки и заявяване на регистри, като със заповед № З-ЦУ-1782/08.12.2020 г. и заповед № З-ЦУ-1830/17.10.2022 г. на

изпълнителния директор на НАП били утвърдени промени и допълнения в предходната 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. По отношение на съхранението и архивирането на електронни документи и документи на хартиен носител в НАП, се прилагали и разпоредбите на актуализираните и утвърдени със заповед № З-ЦУ-2076/06.10.2023 г. на изпълнителния директор на НАП Вътрешни правила за оборот на електронни документи и документи на хартиен носител в НАП, които били 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. С това бил въведен административен ред за унищожаване на електронни документи, вкл. на съдържащите лични данни, данъчна и осигурителна и др. нормативно защитена информация. Фактическото унищожаване на електронни документи се извършвало чрез изтриване след предоставяне на акт за унищожаване от постоянно действаща експертна комисия до определени служители от ИСЕУ. Със заповед № З-ЦУ-2659/21.12.2023 г. на изпълнителния директор на НАП били утвърдени Указания за предоставяне на нормативно защитена информация, в случаите в които се оформя като приложения към кореспонденцията, водена от НАП, които регламентирали реда и начина за защита чрез технически средства на MSOffice на приложения, съдържащи лични данни, данъчна, осигурителна и др. нормативно защитена информация при изпращане по електронен път на външна кореспонденция, водена от НАП. Указанията били задължителни за всички служители.

Съдът не може да установи наличието на въведените с посочените от жалбоподателя в изпълнение на разпореждане № 17 правила документи, както и как същите сработват, поради което изпълнението и на това разпореждане следва да бъде предмет на последваща проверка за изпълнението му. Поради недоказаното наличие на такива правила към момента на произнасяне, съдът приема, че това разпореждане към момента на издаването си е било законосъобразно.

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

Според разпореждане № 18, НАП трябва 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.
Разпореждане № 19 определя като задължение на НАП да актуализира длъжностните характеристики на служителите на НАП с включени клаузи, касаещи обработването на лични данни.
Разпоредбата на чл.38, §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. В разпореждане № 18 е поставено и допълнително изискване, относимо само към длъжностното лице по защита на данните. По делото се установява, че към момента на издаване на оспорения акт това лице е от отдел „Вътрешна сигурност и защита на информацията“, Дирекция „Сигурност“, пряко подчинена на изпълнителния директор на НАП.
В писмените си бележки жалбоподателят твърди, че със заповед № 3740/20.09.2019 г. на основание чл.16 от Закона за държавния служител, считано от 20.09.2019 г. на държавен служител в Дирекция „Сигурност” е възложено временно да изпълнява и длъжността „длъжностно лице по защита на данните”. След проведен конкурс била актуализирана длъжностната характеристика за тази длъжност, утвърдена със заповед № З-ЦУ-1312/10.09.2019 г. на изпълнителния директор на НАП, като последната актуализация на длъжностната характеристика на длъжността „длъжностно лице по защита на данните” била извършена със заповед № З-ЦУ-1098/31.05.2023 г., с която допълнително били регламентирани конкретни задължения, произтичащи от действащото законодателство. Длъжността била подчинена на изпълнителния директор на НАП.
В тази връзка съдът намира, че НАП е изпълнила задължението си по регламент длъжностното лице по защита на данните да се отчита пред изпълнителния директор на НАП, тъй като същият попада в хипотезата на „най-висшето ръководно ниво на администратора или обработващия лични данни.“
Доколкото обаче при новото разглеждане на делото не бяха представени доказателства за твърдяното изпълнение на разпореждания № 18 и 19,

вкл. относно съдържащите се в длъжностната характеристика ясни права и задължения за защита на лични данни от длъжностното лице в съответствие с изискванията на чл.39 от Регламент 2016/679, съдът намира, че към датата на постановяването им тези разпореждания са били законосъобразни.

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.

Според разпореждане № 2, НАП следва да предприеме подходящи технически и организационни мерки с цел повишаване защитата при обработка на лични данни в приложения за електронни услуги към гражданите.

Според разпореждане № 20 - да изготви вътрешни правила за обучение и тренировка на служителите на НАП за действия в случаи на незаконосъобразно обработване на лични данни.

Първата СТЕ по делото е установила, че към датата на изготвянето й НАП е имала утвърден План за непрекъсваемост на дейността и планове за непрекъсваемост на критичните информационни системи. Също така имало 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 Инспектората 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 участвали в тренировки за симулиране действия при инциденти, свързани с работата на информационните системи в НАП, което респективно засягало и неправомерното обработване на лични данни в НАП, като неразделна част от защитата на данъчната и осигурителна информация. Последното известно участие в подобно обучение било през месец април 2019 г. Липсвали обучения за защита на личните данни на целия състав на работещите в НАП служители, а единственият договор бил с Информационно обслужване и Лабораторията за киберсигурност. Обучението за сигурност на данните касаело само малка група от служителите на НАП.

Съгласно втората СТЕ, НАП разполагала с План за непрекъсваемост на дейността и планове за непрекъсваемост на критичните информационни системи, базиран на разработена и внедрена СУСИ по стандарт БДС ISO/IEC 27001/2014. Имало разработени и внедрени процедури за

действие при настъпили инциденти или при наличие на съмнения за такива. НАП провеждала 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 последното било проведено през април 2019 г.

От заключенията по СТЕ се установява, че към момента на издаване на оспореното решение на КЗЛД само част от служителите са участвали в обучения по защита на личните данни, като това са били служители, отговарящи за информационната система, т.е за служителите на IT отдела.

По отношение предприетите технически и организационни мерки, от заключенията на вещите лица и по двете СТЕ се установява, че от страна на администратора на лични данни не са предприети предвидените в чл.32, б.„в" от Регламента 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 била обновявана и адаптирана към непрекъснато изникващите нови заплахи за информационната сигурност. „SQL 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 дължал 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, било технически възможно предотвратяването на изтичане на данни към 2019 година.

Въз основа на тези установявания, може да се направи извод, че администраторът на лични данни НАП 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").

Съгласно разпореждане № 20 и мотивите към него, КЗЛД не отрича факта на провеждането на обучения, а само липсата на процедура и вътрешни правила за тяхното провеждане. Жалбоподателят не е представил доказателства за съществуването на вътрешни правила, а само договори за
извършване на подобно обучение. В писмените бележки на жалбоподателя са посочени много предприети от края на 2020 и началото на 2021 г. действия за обучение на всички служители на Агенцията, касаещо работата с лични данни, регламентирани с конкретни правила. Посочено е също, че с изграждането на новия е-портал за ЕУ на НАП детайлно са били анализирани възможните рискове от злонамерени действия, оказващи въздействие върху нивото на сигурност на интернет страницата на НАП.
Тъй като обаче към момента на постановяване на решението на КЗЛД не е установено наличието на вътрешни правила за провеждане на обучение на служителите на НАП, както и наличието на подходящи технически и организационни мерки с цел повишаване на защитата при обработването на лични данни в приложения за електронни услуги към гражданите, съдът намира, че към датата на постановяването им разпореждания № 2 и № 20 са били законосъобразни.
По изложените съображения жалбата като неоснователна следва да бъде отхвърлена.
При този изход на спора и на основание чл.143, ал.3 от АПК, искането на ответника за присъждане на юрисконсултско възнаграждение следва да бъде уважено. Предвид фактическата и правна сложност на делото, съдът намира, че юрисконсултското възнаграждение следва да бъде определено в максималния размер от 240 лева.
Водим от горното и на основание чл.172, ал.2 от АПК, Административен съд – София град, второ отделение, 30-и състав,

РЕШИ:

ОТХВЪРЛЯ жалбата на Националната агенция за приходите срещу решение № ППН-02-399 от 22.08.2019 г. на Комисията за защита личните данни.
ОСЪЖДА Националната агенция за приходите да заплати на Комисията за защита личните данни сумата от 240 (двеста и четиридесет/ лева, представляваща юрисконсултско възнаграждение.
Решението подлежи на обжалване с касационна жалба в 14-дневен срок съобщаването му на страните пред Върховния административен съд.

Съдия: