1000 София, бул. "Княз Александър Дондуков" № 52 Телефон: 0700 18 700 Факс: (02) 9859 3099

Изх. №94-Б-138#4 от 29.04.2024 г.

ДО

Г-Н ……..

Ел. адрес:……..

ОТНОСНО: Заявление за предоставяне на информация по реда на ***Закона за достъп до обществена информация*** (ЗДОИ) с рег. №94-Б-138 от 22.04.2024 г. по описа на Централно управление (ЦУ) на НАП

УВАЖАЕМИ ГОСПОДИН ……,

В отговор на Ваше Заявление за предоставяне на информация по реда на ЗДОИ, постъпило в ЦУ на НАП с рег. №94-Б-138 от 22.04.2024 г., Ви уведомявам за следното:

Отправено е искане за предоставяне на информация как НАП се справя с кризата предизвикана от изтичането на данни, до колко е била подготвена агенцията за подобна криза, как тази криза е допринесла за подобряването на работата на агенцията, както и всичко друго, което е релевантно към тази тема.

В искането е посочено, че информацията е необходима във връзка с подготовката на дипломна работа по публична администрация на тема: „Възможности за управление на кризи в публичната администрация" в Стопанския факултет на Великотърновския университет „Св. Св. Кирил и Методий". В плана на дипломната работа е заложена за изследване и кризата, предизвикана от изтичането на лични данни на български лица през 2019 г.

В подаденото заявление не е посочена предпочитана форма за предоставяне на достъп до обществената информация, съгласно изискването на чл. 25, ал. 1, т. 3 от ЗДОИ, но е посочен електронен адрес:…….. По аргумент от чл. 35, ал. 3 и чл. 41а, ал. 4 от ЗДОИ, решението ще бъде изпратено на заявителя на посочения от него електронен адрес: …….

Предвид горепосочената цел и вземайки под внимание разпоредбата на чл. 2а, ал. 1 от ЗДОИ, съгласно която „повторно използване на информация от обществения сектор е използването й за търговски или нетърговски цели, различни от първоначалната цел, за която е била създадена в рамките на правомощията или функциите на организация от обществения сектор“, отправеното искане следва да бъде квалифицирано като искане за повторно използване на информация от обществения сектор и да бъдат приложени разпоредбите на чл. 41а и сл. от ЗДОИ.

След преценка на така отправеното искане и на съответните разпоредби на ЗДОИ намирам искането за допустимо и основателно, доколкото се иска предоставянето на достъп до обобщена информация, което няма да доведе до разкриване на данни, защитени от действащото законодателство, по отношение на които ЗДОИ е неприложим.

С оглед изложеното и на основание чл. 41а, ал. 1 от ЗДОИ, Ви предоставям следната налична в НАП информация:

Към 15.07.2019 г., когато е осъществен неоторизиран достъп до информационната система на НАП и са разпространени незаконно лични данни на физически лица, Националната агенция за приходите, като администратор на лични данни, е предприела редица технически и организационни мерки за защита при обработването на лични данни, както следва:

1. В изпълнение на разпоредбата на чл. 24 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*** (ОРЗД), както и на чл. 59, ал.1 ***Закона за защита на личните данни*** (ЗЗЛД), НАП, в качеството си на администратор на лични данни, като е отчитала естеството, обхвата, контекста и целите на обработването, както и рисковете за правата и свободите на физическите лица, е приложила необходимите подходящи технически и организационни мерки, за да гарантира, че обработването се извършва в съответствие с посочените нормативни актове, от една страна и в изпълнение на чл. 32 от ОРЗД относно необходимостта да бъдат предприети конкретни мерки за постигане на сигурност и защита на личните данни в съответствие с достиженията на техническия прогрес. Тези мерки се преразглеждат и при необходимост се актуализират.

Съгласно утвърдените стандарти за информационна сигурност и действащите вътрешни процедури в НАП се извършва надлежно наблюдение и анализ по отношение на непрекъсваемостта, работоспособността, интегритета и бързодействието на информационните системи в НАП. **А*нализират се заплахите за информационната система, ведно с потенциалните уязвимости и при съобразяване със съществуващите мерки. Анализ на риска за всички системи се извършва в рамките на общата оценка на риска за информационните активи, съгласно утвърдените в НАП процедура и методика за оценка на риска за информационната сигурност***.

В НАП се използват съвременни средства за антивирусна защита и тестване за уязвимости на ИС от световно доказани производители в различните области. Наличните информационни системи и предлагани информационни услуги са **съобразени с „достиженията на техническия прогрес“,** както към момента на узнаване за извършения неоторизиран достъп до база данни на НАП, така и преди влизане в сила на ОРЗД (в сила от 25.05.2018 г.).

Следва да се отбележи също така че НАП води „чиста“ лицензионна политика и използва хардуерни и софтуерни продукти, доставени само от производители и/или техни оторизирани партньори. В тази връзка в Агенцията винаги са се използвали технически средства и софтуер, съобразени със съвременни средства за защита в сферата на администриране и поддръжка на информационните системи и бази данни.

В Агенцията са прилагани всички организационни мерки, съгласно изискванията на относимото към момента на узнаване за извършения неоторизиран достъп законодателство. Политиките, правилата, процедурите и инструкциите, свързани с жизнения цикъл на информационните системи са част от внедрената в НАП през 2014 г. **Система управление на сигурността на информацията** (СУСИ), утвърдена със Заповед №З-ЦУ-586 от 30.04.2014 г. на изпълнителния директор на НАП.

Същите се актуализират своевременно в съответствие с измененията в действащите нормативни актове. Следва да се има предвид, че ***Законът за киберсигурност*** влиза в сила в края на 2018 г. (ДВ. бр.94 от 13 ноември 2018 г.), а ***Наредбата за минималните изисквания за мрежова и информационна сигурност*** (НМИМИС), приета на основание чл. 3, ал. 2 от ***Закона за киберсигурност*** с ПМС №186 от 19.07.2019 г, е в сила от **26.07.2019г.,** т.е. към момента на извършване на неоторизирания достъп, действащите процедури и правила в НАП са били съобразени с нормативните изисквания, съгласно действащата редакция на разпоредбите на ***Закона за електронното управление*** (ЗЕУ) от

2018 г., ***Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги*** (НОИИСРЕАУ) от 2017 г. и отм. ***Наредба за общите изисквания за мрежова и информационна сигурност (НОИМИС)*** с последни изм. и доп. от 17 януари 2017 г.

Като допълнителни доводи по отношение на верификацията на прилаганите организационни и технически мерки от НАП, следва да отбележим и одитите, които бяха извършени по линия на The Automatic Exchange of Information (AEOI) /*автоматичният обмен на информация*/, Common Reporting Standard (CRS) /Общият стандарт за предоставяне на информация/ и Foreign Account Tax Compliance Act (FATCA) */Актът за спазване на данъчното законодателство във връзка със задгранични сметки/,* с цел установяване дали Агенцията отговаря на минималните изисквания за информационна сигурност и дали е „надежден“ партньор при предоставяне на електронни услуги и осъществяване на автоматичен обмен на данни и информация с държавите-членки на ЕС.

Тези одити са извършени както чрез документална проверка – попълване на Въпросници за информационна сигурност от страна на НАП, така и чрез проверка на място от представители на компетентните международни органи.

В резултат на одитите не са констатирани несъответствия и отклонения, както и не са отправяни съществени препоръки за корекции в прилаганите организационни и технически мерки по отношение на нивото на информационна сигурност в НАП.

В допълнение на изложеното, относимо е и обстоятелството, че през 2018 г. в резултат на извършена проверка (в периода 17-20.09.2018 г.) от ***Държавна агенция „Електронно управление“*** (ДАЕУ) като орган осъществяващ контрол, на основание чл. 59 от ***Закона за електронно управление*** (ЗЕУ) по спазване на нормативните изисквания за мрежова и информационна сигурност (МИС) от административните органи, съгласно ЗЕУ, респ. изискванията за мрежова и информационна сигурност и оперативна съвместимост съгласно отм. НОИМИС и съответно НОИИСРЕАУ, и предвид влизането в сила на ***Закона за киберсигурност*** (м. ноември 2018 г.), **не са установени нарушения от страна на ДАЕУ (правоприемник – Министерство на електронното управление) при прегледа на текущото състояние на МИС, информационните ресурси, свързани с всички регистри, бази данни и информационни системи, поддържани и администрирани от НАП.**

Неоторизираният достъп до данни на НАП е причинен вследствие на престъпно, съгласно ***Наказателния кодекс*** на Република България, действие, без оглед на предприетите мерки за сигурност, а въпреки тях (арг. чл. 82, параграф 3 от ***Регламент***

2016/679). В качеството си на администратор, НАП доказа, че този факт не може по никакъв начин да бъде вменен на агенцията, тъй като не е отговорна за събитието, причинило вредата.

2. Във връзка с осъществения неоторизиран достъп до информационната система на НАП и неправомерното разпространение на лични данни е важно да се подчертае, че в резултат на посегателството са засегнати **частични данни за определени физически или юридически лица**. Следва да се има предвид, че компрометираните данни не са пълни или валидни във всички случаи. Освен това, тези данни не са били разкрити в четим формат, под формата на електронни документи, а са необходими допълнителна обработка и специфични компютърни знания, за да бъде възстановен набора от данни, наличен за даден данъкоплатец. Липсва механизъм, чрез който да се докаже по безспорен начин, че определени данни са станали обект на неторизиран достъп, чрез осъществен такъв именно до конкретен документ, съхраняван в НАП.

В изпълнение на изискванията на чл. 33 и чл. 34, ал. 3, букви „б“ и „в“ от Регламент (ЕС) 2016/679, НАП незабавно след узнаването за осъществения нерегламентиран достъп до информационните й системи, предприе мерки за преустановяване на неоторизиран достъп до лични данни и действия за уведомяване на Центъра за действие при инциденти в информационната сигурност в ДА „Електронно управление“ (съгл. чл. 21 от ***Закона за киберсигурност***) и специализираните звена в ДА „Национална сигурност“ и ГД „Борба с организираната престъпност“ в МВР. С писма на изпълнителния директор на НАП са уведомени също Комисията за защита на личните данни (КЗЛД) за извършеното нарушение на сигурността на личните данни и Софийска градска прокуратура за образуване на наказателно производство. Предприетите са незабавни действия и за информиране на засегнатите физически лица и партньорите на Агенцията – Министерство на вътрешните работи, Министерство на труда и социалната политика, Главна дирекция „Гражданска администрация и административно обслужване“ към МРРБ, Агенция по вписванията, Агенция по заетостта, Агенция за социално подпомагане, Агенция „Митници“ и др. Своевременно са изпратени съобщения и нота до Европейската комисия и са уведомени съответните структури на Организацията за икономическо сътрудничество и развитие и партньорските юрисдикции на България в областта на данъчното сътрудничество за неоторизирания достъп в базите данни на НАП.

По отношение приложението на разпоредбите на чл. 34 от Регламент (ЕС) 2016/679 и на чл. 68 от ЗЗЛД относно информирането на субектите на данни за нарушение на

сигурността на личните им данни, в резултат на осъществения неоторизиран достъп до информационната система на НАП, изпълнителният директор на НАП, на основание чл. 10а, ал. 2, т. 2 от ЗЗЛД поиска от Комисията за защита на личните данни (КЗЛД) да изрази становище по този въпрос, с цел предприемане на законосъобразни действия от страна на Агенцията. В отговор, с писмо на председателя на КЗЛД, се произнесе, че „…**Предвид броя на засегнатите физически лица и обема на лични данни с нарушена сигурност, може обосновано да се приеме, че в настоящия случай е приложима хипотезата на буква „в“ от същия (в случая - чл. 34, пар.3, б. „в“ от Регламент (ЕС) 2016/679) – когато изпращането на индивидуалните съобщения би довело до непропорционални усилия, в който случай Общият регламент въвежда изискването за публично съобщение или друга сходна мярка, така че субектите на данни да бъдат в еднаква степен информирани…“.**

3. Тъй като НАП обработва голям брой данни, попадащи в обхвата на информация, защитена от закон - като лични данни, данъчна и осигурителна информация, информация за вътрешно ползване, ограничено ползване и конфиденциална информация, в Агенцията се прилагат действащите политики, правила, процедури, указания и методики за управление на сигурността на информацията в НАП по отношение на всички защитени данни.

Вътрешните документи, имащи отношение към информационната сигурност и утвърждавани от изпълнителния директор на НАП, са съобразени с изискванията на ***Закона за електронно управление (ЗЕУ), Наредбата за общите изисквания към информационните системи, регистрите и електронните административни услуги (НОИИСРЕАУ) и Наредбата за общите изисквания за мрежова и информационна сигурност (отменена на 26.07.2019 г.).***

В указанието за обозначаване и работа с информация, утвърдено от изпълнителния директор на НАП, е предвидено, че информация, съдържаща лични данни се маркира с „Ограничено ползване“ и са предвидени надлежните организационни и технически мерки за работа с нея.

Правилата и процедурите, утвърдени в НАП, свързани с обработването на лични данни, са задължителни за изпълнение от всички служители на НАП.

Следва да отбележа, че Вътрешните правила не са общи, а регламентират конкретните задължения на служителите на НАП. Те са в съответствие със стандартите и

добрите практики за постигане на сигурност на информацията, обработвана в НАП от служителите ѝ.

3. Всички привилегировани потребители в НАП са поименно определени със заповед на изпълнителния директор на НАП и достъпват информационните ресурси на НАП, съобразно длъжностната си характеристика и на принципа „необходимо е да се знае“.

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

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

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

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

Не на последно място, в НАП е утвърдена **Процедура за оценка на риска за сигурността на информацията** и **Методика за оценка на риска за сигурността на информацията към процедурата**, която обхваща последователността от действия и отговорностите за провеждане на оценка на риска за сигурността на информацията, в съответствие с установената Политика за управление на риска (т. 7 на **Политика по**

информационна сигурност на НАП). В методиката и разработените и утвърдени форми за оценка на риска са идентифицирани заплахите и способите за оценка на риска, които са приложими към всяка една информационна система на всички етапи на нейния жизнен цикъл. В НАП се извършват оценки на риска, при първоначално въвеждане в експлоатация на нови системи, при промяна на системата и периодично, организирано от звеното по мрежова и информационна сигурност.

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

Правилата и процедурите, утвърдени в НАП, свързани с обработването на данните в данъчно-осигурителната сметка, включително и специфични данни, свързани с данъчните и осигурителните задължения, са същите, с които се обработват всички данни в информационните системи като неразделна част от данъчната и осигурителната информация и са задължителни за изпълнение от всички служители на НАП.

5. Следва да се има предвид, че на официалната интернет страница на НАП в рубрика „За НАП“, подрубрика „Основни документи“ бе публикувана ***„Политика за защита на личните данни в Националната агенция за приходите“***, утвърдена със Заповед №ЗЦУ-746/25.05.2019 г. на изпълнителния директор на НАП, в която са посочени имената и телефоните за контакти на длъжностните лица за защита на данните за Централно управление на НАП и за Териториалните дирекции на НАП. За информация по отношение на осъществения неоторизиран достъп до информационната система на НАП, гражданите можеха да се обръщат и към Информационния център на НАП на тел. 0700 18 700. В тази връзка, всеки който е потърсил нужната му информация е получил същата. Откритият и прозрачен диалог при информиране на обществеността относно извършената кибератака цели всеки гражданин да разбере, че НАП полага всички усилия извършеното компютърно престъпление да не бъде основа за извършване на нови престъпления.

Чрез поредица от медийни събития НАП информира и комуникира с обществеността честно и открито по отношение на проблема с неправомерното разпространение на данни. Обслужени са няколко хиляди клиенти, изготвени са отговори на множество постъпили писма и жалби, като **водещ принцип е заедно да се справим, уважавайки емоциите на засегнатите лица.** Информирани са физическите

лица с най-голям обем достъпена информация за нарушаване сигурността на личните им данни, независимо, че достъпената информация е частична и за да се използва злонамерено е необходимо да бъде допълнително обработена.

С цел безпрепятствено упражняване на правото на гражданите да бъдат своевременно информирани, непосредствено след узнаване за нарушението, НАП разработи специално приложение, чрез което **всеки български гражданин да може да провери дали негови лични данни са станали обект на неоторизиран достъп**, след въвеждане на ЕГН и номер на мобилен телефон, както и да получи информация за техния конкретен вид (вкл. да направи разпечатка на справката). Освен чрез приложението, гражданите можеха да получат информация и във всички офиси на НАП след идентификация с документ за самоличност.

С цел публичност и открита комуникация на интернет страницата на НАП бе създадена **специализирана рубрика „Разпространени данни на НАП“**, в която своевременно се публикуваше актуална информация по всички въпроси, свързани с незаконно разпространените лични данни. Наред с това НАП предприе редица мерки за ограничаване и преодоляване на неблагоприятните последици от извършеното нарушение, засегнало сигурността на личните данни на гражданите.

Като основна превантивна мярка, която целеше да предотврати потенциална злоупотреба и неправомерно използване на незаконно разкрити лични данни, Агенцията оповести публично препоръките към своите клиенти. В сътрудничество с държавни, банкови и финансови институции, нотариуси и др. като Агенцията по вписванията, Нотариалната камара, Асоциацията на банките в Република България, дружества за бързи кредити и лизинг, своевременно са предприети достатъчно надежди мерки за проверка при идентификация, за да се гарантират интересите и имуществото на всеки български гражданин, чиито лични данни са разпространени незаконно.

В сайта на Агенцията бяха създадени специални рубрики, свързани с кибератаката към НАП, в които своевременно се публикуваше актуална информация. Експерти от НАП, нотариуси и финансисти разработиха отговори на **най-често задаваните въпроси** във връзка с нерегламентирания достъп до данни, както и съвети към гражданите, чиито данни са разпространени.

Националната агенция за приходите засне кратък **информационен видеофилм със съвети и отговори на най-често задавани от гражданите въпроси за действия,**

които трябва или не е необходимо да бъдат предприети след осъществения неоторизиран достъп до информация, съдържаща се в част от базите данни на НАП.

Всички горепосочени мерки, както и ежедневните изявления в средствата за масово осведомяване са предприети от НАП с цел да се защитят максимално правата на гражданите, да се успокои обществеността и да се преодолее неоснователният страх от евентуални злоупотреби с лични данни и данъчна и осигурителна информация. В резултат на положените извънредни усилия от страна на органите и служителите на НАП, в условията на извънреден труд, непрекъснато напрежение и стрес, **НАП не допусна да бъде нарушено общественото доверие към нея като специализиран държавен орган**, който допринася всекидневно със своя труд за просперитета на Република България, въпреки извършения неоторизиран достъп до информационната й система.

Предвид разпоредбата на чл. 41а, ал. 4 от ЗДОИ, информацията ще Ви бъде изпратена своевременно по електронна поща на посочения в заявлението електронен адрес:……., без да се дължат суми по предоставянето й.

ЗА ИЗПЪЛНИТЕЛЕН ДИРЕКТОР НА НАП:
/МИЛЕНА КРЪСТАНОВА/

(Съгласно Заповед №ЗЦУ-ОПР-12 от 09.04.2024 г.
на изпълнителния директор на НАП)

Документът е електронно създаден и подписан, като данни за електронния подпис на издателя се визуализират в горния десен ъгъл на началната страница, съгласно действащите нормативни изисквания.

*Национална агенция за приходите обработва и защитава личните Ви данни, съобразно изискванията на **Закона за защита на личните данни (ЗЗЛД)** и Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г.*

Повече подробности за ангажиментите на Националната агенция за приходите, в качеството ѝ на администратор на лични данни, можете да намерите в ***„Политика по защита на личните данни в Националната агенция за приходите“****, публикувана на интернет адрес: www.nra.bg или да се свържете с нас на имейл адреса на Информационния център на НАП: infocenter@nra.bg* и телефон: *0700 18 700.*