АСОЦИАЦИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

www.mydata.bg

ДО

МИНИСТЪРА НА ФИНАНСИТЕ

ДО

ИЗПЪЛНИТЕЛНИЯ ДИРЕКТОР НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ

З А Я В Л Е Н И Е
ЗА ДОСТЪП ДО ОБЩЕСТВЕНА ИНФОРМАЦИЯ

от Сдружение „Асоциация за защита на личните данни“,
ЕИК: 177186262, със седалище и адрес на управление: гр. София, 1113, ул. „Д-р Любен Русев“ № 36, вх. Г, ет. 2, ап. 36, представлявано от Юлия Пригонча – председател на Управителния съвет

телефон за връзка: 0899986018, 0886013569,
ел. поща: dpa.bulgaria@mydata.bg

УВАЖАЕМИ ГОСПОДИН МИНИСТЪР,
УВАЖАЕМА ГОСПОЖО ИЗПЪЛНИТЕЛЕН ДИРЕКТОР,

Асоциация за защита на личните данни е сдружение с нестопанска цел, което обединява експерти от различни професионални направления в областта на защитата на личните данни и работи активно за да развие, популяризира и утвърди основните принципи, успешните модели и добрите практики за защита на личните данни; да повиши осведомеността на обществото по тази изключително важна тема; да подпомогне компаниите и организациите при постигането и поддържането на съответствие с изискванията на законодателството и да насърчи и съдейства на хората да упражняват своите права.

Силно сме обезпокоени от изнесената в медиите информация на 15.07.2019 г. за извършена хакерска атака срещу информационните системи на Министерството на финансите (МФ) и Националната агенция по приходите (НАП), в резултат на която хакери са придобили и разпространили данни на над 5 милиона граждани и фирми.

Голяма част от тези данни представляват лични данни съгласно дефиницията на чл. 4, т. 1 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното

движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент за защита на данните, ОРЗД).

Във връзка с настъпилия инцидент и задълженията, които ръководените от Вас публични институции, в качеството си на администратори на лични данни, имат по посочения Регламент и по Закона за достъп до обществена информация (ЗДОИ), молим за отговор и информация по следните направления:

I. Публикуване на информация за извършените от МФ и НАП оценки на въздействие и направените основни констатации

Разпоредбите на чл. 6, пар. 1, б. „е“, чл. 24 и чл. 32 от ОРЗД задължават администраторите на лични данни, вкл. и тези от публичния сектор, да въвеждат и прилагат подходящи технически и организационни мерки за защита на личните данни.

Прилагането на подходящи мерки се осъществява в резултат на извършени анализи от страна на администраторите, които включват и оценка на рисковете от всяка дейност по обработване за правата и свободите на физическите лица – субекти на данни.

В чл. 35 от ОРЗД се въвежда понятието за оценка на въздействието върху защитата на данните (ОВЗД). ОВЗД представлява процес, чиято цел е да опише дейностите по обработване на лични данни, да оцени тяхната необходимост и пропорционалност и да спомогне за управлението на рисковете за правата и свободите на физическите лица, произтичащи от това обработване, като ги оцени и определи мерки за справяне с тези рискове.

От гледна точка на управлението на риска ОВЗД е насочена към управление на рисковете за правата и свободите на физическите лица, като се използват следните процеси:

- установяване на контекста – взимат се предвид естеството, обхвата, контекста и целите на обработването на лични данни, както и източниците на риска;

- оценка на рисковете – оценяват се конкретната вероятност и тежестта на високия риск;

- третиране на рисковете – предприемат се мерки за ограничаване на тези рискове, с които да се осигури защитата на личните данни и да се доказва съответствието с ОРЗД.

Трябва да се подчертае, че с цел управление на рисковете за правата и свободите на физическите лица, тези рискове трябва редовно да се идентифицират, анализират, преценяват, оценяват, третират (например като се ограничават и своевременно се отстраняват предпоставките за възникването им) и преразглеждат. На практика това означава, че администраторите трябва непрекъснато да провеждат процес по оценка на рисковете, които се пораждат от техните дейности по обработване, за да идентифицират кога съществува вероятност определен вид обработване „да породи висок риск за правата и свободите на физическите лица“, както е казано в чл. 35, пар. 1 от ОРЗД.

Съгласно ОРЗД неспазването на изискванията за извършване на ОВЗД може да доведе до налагане на глоби от компетентния надзорен орган. Ако не бъде извършена ОВЗД, когато обработването подлежи на ОВЗД (чл. 35, пар. 1, 3 и 4 от ОРЗД), ако ОВЗД бъде извършена неправилно (чл. 35, пар. 2, 7 и 9 от ОРЗД) или ако не бъде проведена консултация с

компетентния надзорен орган, когато това се изисква (чл. 36, пар. 3, б. „д“ от ОРЗД), това може да доведе до налагането на глоба в размер до 10 милиона евро или, в случай на предприятие, до 2 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока.

ОВЗД представляват важен инструмент за отчетност, тъй като помагат на администраторите на лични данни не само да спазват изискванията на ОРЗД, но и да демонстрират, че са предприели подходящи мерки за гарантиране на спазването на Регламента и за защита на правата и свободите на субектите на данни.

Според чл. 35, ал. 1 от ОРЗД отговорност за извършване на оценката носи администраторът на лични данни.

Съгласно становището на Работната група по защита на личните данни към Европейската комисия (Европейски комитет по защита на данните, считано от 25.05.2018 г.) *„Особено добра практика е да се публикува ОВЗД, когато гражданите са засегнати от операцията по обработване. Такъв би могъл да бъде случаят по-специално когато публичен орган извършва ОВЗД“* и *„Целта на този процес е да се подпомогне изграждането на доверие в извършваните от администратора операции по обработване и да се демонстрира отчетност и прозрачност“*.

Предвид гореописаните важни аспекти и ползите от извършването на оценките на въздействие, липсата на пречка тази информация да е публично достъпна, необходимостта от възстановяване на доверието в ръководените от Вас институции, като се покаже и докаже на физическите лица резонността на приложените мерки, а и на основание чл. 14, ал. 2 от ЗДОИ и цитираните по-горе насоки на Работната група (сега Европейски комитет по защита на данните), настояваме МФ и НАП да публикуват тази информация (извършените оценки на въздействие) на Интернет страниците си незабавно.

Молим копия от извършените от МФ и НАП оценки на въздействието върху защитата на личните данни да ни бъдат предоставени по реда на ЗДОИ, а в случай че не могат да ни бъдат дадени в цялост, молим да ни бъде изпратена обобщена информация за резултатите от тях.

II. Изпращане на информация към физическите лица от страна на Длъжностните лица по защита на данните

Съгласно чл. 37, пар. 1, б. „а“ от ОРЗД публичните институции са длъжни да определят Длъжностно лице по защита на данните. Длъжностното лице по защита на данните има важна роля и подпомага администратора на лични данни при осъществяване на неговата дейност, така че правата на субектите на данни да са защитени. Т.е това е един вид „пазител“ на тези данни. Допълнително ОРЗД въвежда изсквания за извършване на непрекъснат одит и мониторинг на спазването на изискванията на закона и въведените от администратора вътрешни политики,

процедури и правила, в който процес основна роля играе Длъжностното лице по защита на данните.

Във връзка с тези важни функции, възложени на Длъжностното лице по защита на личните данни, и в духа на принципа за прозрачност, скрепен в чл. 5, пар. 1 б. „а“ от ОРЗД, както и на основание чл. 14, ал. 2 от ЗДОИ, настояваме на Интернет страниците на МФ и НАП да бъде публикувана информация за наличния процес в МФ и НАП за мониторинг по ОРЗД, честотата на проверките, приложените мерки, предприетите действия и основните констатации и препоръки, отправени към МФ и НАП като администратори на лични данни от страна на Длъжностните лица по защита на данните, включително становищата им във връзка с описания по-горе инцидент.

Независимо от това дали тази информация ще бъде публикувана на Интернет страниците на МФ и НАП, молим тя да ни бъде предоставена по реда на ЗДОИ.

III. Превенция и ограничаване на последствията от инцидента

В съответствие с подхода, базиран на риска, предвид естеството, мащаба и броя засегнати лица, настояваме на основание чл. 14, ал. 2 от ЗДОИ МФ и НАП да публикуват на Интернет страниците си и анализ и оценка на евентуалните рискове за правата на субектите на данни, които могат да се реализират в резултат на настъпилия инцидент, за да могат тези рискове да бъдат разпознавани от физическите лица и те да могат да се предпазят от тях.

Молим също така тази информация да ни бъде предоставена по реда на ЗДОИ.

Желаем да получим исканата информация в горните точки под формата на копие на технически носител – по електронна поща на dpa.bulgaria@mydata.bg.

С оглед на това че заявлението се подава по електронен път на посочените от Вас в сайта Ви електронни адреси, на основание чл. 24, ал. 2 от ЗДОИ не е необходимо то да бъде подписано с електронен подпис.

Молим, след завеждане на заявлението във всяка от институциите – адресати, неговият входящ номер да ни бъде изпратен на dpa.bulgaria@mydata.bg.

Заявлението е адресирано едновременно до МФ и НАП, които са самостоятелни администратори на лични данни по смисъла на ОРЗД и задължени субекти по чл. 3 от ЗДОИ, поради което очакваме предприемане на действия и отговори по него от страна и на двете институции.

гр. София
16.07.2019 г.

С уважение,
/Юлия Пригонча – председател на УС/