О П Р Е Д Е Л Е Н И Е
№

гр. София, 04.03.2020 г.

АДМИНИСТРАТИВЕН СЪД - СОФИЯ-ГРАД, **Второ отделение 50 състав,**
в закрито заседание на 04.03.2020 г. в следния състав:

СЪДИЯ: Весела Николова

като разгледа дело номер **10477** по описа за **2019** година докладвано от съдията, и за да се произнесе взе предвид следното:

В срока за произнасяне по съществото на спора, съдът установи, че делото не е изяснено от фактическа страна. За да прецени законосъобразността и правилността на съдържащите се в оспорения административен акт констатации и разпореждания на административния орган, съдът следва служебно да назначи експертиза, предвид необходимостта от специални знания в областта на „Информационната сигурност“.

Предвид изложените съображения, съдът следва да върне делото за разглеждане в открито съдебно заседание с призоваване на страните. Следва да задължи жалбоподателя да внесе депозит за възнаграждение на вещо лице в определен от съда размер.

Ръководен от гореизложеното и на основание чл. 253 от ГПК във връзка с чл. 144 от АПК, съдът

О П Р Е Д Е Л И :

ОТМЕНЯ определение от открито съдебно заседание на 10.12.2019г., с което е даден ход на делото по същество.

НАСРОЧВА открито съдебно заседание на 12.05.2020г. от 15.15часа.

НАЗНАЧАВА съдебно-техническа експертиза с вещо лице Ю. А. Й. от Списъка на вещи лица при СГС и АССГ, тел. [ЕГН], със специалност „Електронна и комуникационна техника и технологии. Достъп до класифиц. информация. Разследване на престъпления в киберпространството“, което след като се запознае с материалите по делото и извърши проверка на съхраняваната документация и поддържаните информационни системи в НАП, да даде заключение като отговори на следните въпроси:

Към датата на неоторизирания достъп и разпространението на личните данни на

15.07.2019г.:

1. Имало ли е създадени конкретни правила за обработка на личните данни в отделните поддържани в НАП информационни системи и мерки за защита на различните категории лични данни, като цяло и съобразно техния вид и чувствителност /съобразно оценката на риска/ ?

2. Имало ли е неограничен достъп на т.н. „привилегировани потребители“ до целия информационен ресурс, ако е имало ограничаване на права – в каква степен и обем са били те и в какво конкретно са се изразявали? Взети ли са били мерки за въвеждане в активната директория на правила за достъп на отделните групи потребители до информационните системи?

3. Имало ли е одитни записи на отделните събития и дневници (журнали) за привилегированите потребители? Имало ли е внедрена Система за управление на привилегиите на потребителите (P. Access M., PAM), с оглед контрол, управление и наблюдение на привилегирован достъп до критични активи? Внедрена ли е била Система за управление и анализ на събитията, отразени в дневниците (S. information and event management, S.), 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? Вещото лице да провери лок-файловете за какъв период от време се съхраняват и за кои операции се съхраняват ?

4. Имало ли е създадена 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 ?

5. Извършван ли е бил анализ на риска на системите и операциите по обработването, включващи изготвени правила и функционални задължения за работа на всяка информационна система ?

6. Извършвана ли е била оценка на въздействието при идентифициран „висок риск” за всяка една система и предприетите мерки (съгласно одобрен и публикуван на интернет страницата на КЗЛД списък на по чл. 35, параграф 4 от Регламент (ЕС) 2016/679) ?

7. Имало ли е документирани правила за оценка на въздействието при защита на данните при първоначално стартиране на нови информационни системи и приложения ?

8. Стартирана ли е била процедура по адаптиране на информационните системи към изискванията на Регламент (ЕС) 2016/679 ? Създадени ли са били правила за управление на риска при въвеждане на нови системи или промяна на вече съществуващи системи (P. By D., P. By R. и P. By D.) ?

9. Предприети ли са били действия за обновяване на операционните системи от W. 2008R2 към актуални версии от 2013 г. и 2016 г., и на СУБД O. 11.2.0.2 към актуална версия O. 12, за осигуряване сигурността на данните след 2020 г., когато изтича срокът за тяхната поддръжка ?

10. Имало ли е изграден център за възстановяване работоспособността на системите в реално време (D. R. C.) и ако е имало такъв, дали е осигурявал само резервираност на данните или е осигурявал също и предпазване и защита срещу нерегламентиран достъп ?

11. Създадени и прилагани ли са били правила и мерки за: обработване на специални

категории данни съгласно чл. 9 от Регламент (ЕС) 2016/679; за повторно използване на личните данни на субектите; за анонимизиране, архивиране и унищожаване на електронните данните, използвани еднократно (различни видове справки и заявки); за обработка на лични данни на деца, повторното използване на такива данни, проследяващи механизми и С. (бисквитки), определяне срока за съхранение и задържане на данните; извършвало ли се е криптиране на данни от архивни или еднократно извършвани справки ?

12. Имало ли е звено /отделно от IT – звеното/, отговарящо за управление на риска, респективно за защита на данните, което да е на пряко подчинение на изпълнителния директор ?

13. Имало ли е създаден план за действие при операционно събитие, т.е. при нерегламентиран достъп ? Извършвано ли е било обучение на служителите на НАП за реакция в случаи на незаконосъобразно обработване на лични данни ?

УКАЗВА на вещото лице да представи заключението си 7 дни преди насроченото о.с.з.

УКАЗВА на жалбоподателя в 7-дневен срок от съобщаването да внесе депозит в размер на 600лв. за възнаграждение на експерта.

Определението не подлежи на обжалване.

Да се призоват страните и вещото лице за насроченото открито съдебно заседание.

Определението не подлежи на обжалване.

СЪДИЯ: