КОМИСИЯ ЗА ЗАЩИТА
НА ЛИЧНИТЕ ДАННИ

София 1592,
бул. „Проф. Цветан Лазаров" 2
тел.: 02/915 35 15
факс: 02/915 35 25
e-mail: kzld@cpdp.bg
www.cpdp.bg

С Т А Н О В И Щ Е

НА

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

рег. № ППН-02-463/2021 г.

гр. София, 18.11.2021 г.

ОТНОСНО: *Фигурата на длъжностно лице по защита на данните в контекста на служебното правоотношение*

Комисията за защита на личните данни (КЗЛД) в състав – председател: Венцислав Караджов и членове: Цанко Цолов, Мария Матева и Веселин Целков, на заседание, проведено на 10.11.2021 г., разгледа писмо вх. № ППН-02-463/04.10.2021 г. от адвокат от САК, с което моли комисията да установи дали и в каква степен *Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация* противоречи на императивни правила и законни цели установени с Общия регламент относно защитата на данните, и пряко нарушава законоустановената независимост на длъжностно лице по защита на личните данни при изпълнение на неговите задачи.

Във връзка с искането си, адвокатът посочва мотиви и бележки по приложимите правни актове, като изразява притеснение за колизия между тях, както следва:

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета въведе фигурата на длъжностното лице по защита на данните (ДЛЗД). Нейните основни функции са предоставяне на съвети и консултации в областта на защитата на личните данни, както и осъществяване на надзор по спазването на Регламента в организацията на администратора. Член 39, параграф 1 от Регламента посочва изчерпателно задължителен минимум от задачи, които ДЛЗД трябва да изпълнява:

- **да информира и съветва** администратора или обработващия лични данни и служителите, които извършват обработване;
- **да наблюдава спазването** на регламента;
- **при поискване да предоставя съвети** по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно член 35;
- **да си сътрудничи с надзорния орган;**

– **да действа като точка за контакт за надзорния орган.**

За да гарантира безпрепятственото и независимо упражняване на тези специфични и законоустановени надзорни функции, Общият регламент съдържа следните императивни правила установени в чл. 38, пар. 3:

Администраторът и обработващият лични данни правят необходимото длъжностното лице по защита на данните **да не получава <u>никакви</u> указания за тези задачи; и**

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.

Когато обработването се извършва от публичен орган, ОРЗД го задължава безусловно да определи длъжностно лице по защита на данните, независимо от това дали основните му дейности предполагат редовно и/или мащабно обработване на лични данни – чл. 37, пар. 1, б. „а". Вероятно, една от причините за това е, че за разлика от търговското дружество, при публичния орган предвидените в Регламента имуществени санкции не биха имали същия възпиращ и дисциплиниращ ефект. Ето защо, Регламентът изисква публичният орган винаги да бъде подпомаган при наблюдението на вътрешното спазване от лице с експертни познания. В изпълнение на това изискване, с постановление на Министерски съвет, е изменен и допълнен *Класификатора на длъжностите в администрацията,* като е добавена длъжността – *длъжностно лице по защита на личните данни* за всеки един вид администрация.

Към настоящия момент, всяка българска администрация, в изпълнение на задължението си по чл. 37, пар. 1, б. „а", е назначила длъжностно лице по защита на личните данни. В голямата си част, тези лица са назначени на държавна служба и имат статут на държавни служители. По този начин, върху служебното правоотношение възникнало по силата на акта за назначаване и уредено от Закона за държавния служител, се наслагва друго специфично правоотношение, възникващо по силата на Общия регламент - правоотношение между Администратор (Обработващ) лични данни и неговото ДЛЗД. Тоест, и за двете страни възникват поредица от права и задължения, произтичащи от два различни източника - Закона за държавния служител и свързаните с него подзаконови нормативни актове и Регламент (ЕС) 2016/679, Закона защита на личните данни, и други нормативни актове в областта на защитата на данните.

Такъв подзаконов нормативен акт е *Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация*. По тази наредба, ежегодно, се извършва оценяването на изпълнението на длъжността на всеки един държавен служител в съответната администрация, включително и на длъжностното лице по защита на данните,

ако същото е назначено на служебно правоотношение. Оценяването съдържа две компоненти: постигането на предварително определените цели и показаните компетентности. Въз основа на степента на постигане на целите и на показаните компетентности, оценяващият ръководител определя годишната оценка на изпълнението на длъжността, като тази оценка по-нататък служи за определяне на възнагражденията на служителите, за повишаването им в ранг, а при оценка „неприемливо изпълнение" може да бъде законно основание за прекратяване на служебното правоотношение, тоест за уволнението на служителя. Също така, въпросната наредба предвижда провеждането на междинни срещи между оценяващият ръководител и оценяваният, на които се прави преглед на изпълнението на длъжността, **показаните компетентности от служителя,** както и може **да се набележат конкретни действия за подобряване на изпълнението.**

При така изложените аргументи, адвокатът се обръща към КЗЛД, като счита, че извършването на „оценяване на изпълнението на длъжността" заемана от ДЛЗД и „набелязването на конкретни действия за подобряване на изпълнението" на задачите на ДЛЗД от страна на Администратора (Обработващия), представлява нормативно установен способ за санкциониране и освобождаване от длъжност, както и възможност за даване на указания на длъжностното лице как да изпълнява своите задачи. На практика, поднадзорното лице дава оценка на експертизата на извършващото надзора лице, а при незадоволителна оценка му налага санкции.

С оглед всичко гореизложено, адвокатът моли КЗЛД **да установи дали и в каква степен Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация противоречи на императивни правила и законни цели установени с Общия регламент, и пряко нарушава законоустановената независимост на длъжностно лице по защита на личните данни при изпълнение на неговите задачи.**

В допълнение адвокатът отбелязва, че компрометираната самостоятелност на длъжностното лице означава невъзможност за осъществяване на независим надзор върху съответния публичен орган, което пък от своя страна се явява сериозен източник на риск за правата и свободите на субектите данни. Този риск нараства многократно в условията на пандемия, когато множество български публични органи извършват редовно мащабно обработване на специални категории данни – такива относно здравето, както на българските граждани, така и на граждани на държави-членки на ЕС.

Адвокатът също така моли настоящето писмо да се счита за сигнал по реда на Глава осма, Раздел I от АПК, както и моли да бъде уведомена своевременно за решението на КЗЛД по него.

Правен анализ:

Настоящото искане съдържа принципни въпроси по прилагането на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД) в частта му, касаеща правното положение на длъжностното лице по защита на данните (ДЛЗД), които следва да бъдат разгледани в съответствие с чл. 57, пар. 1, б. „в" във връзка с чл. 58, пар. 3, б. „б" от Регламент (ЕС) 2016/679. Тъй като в искането не е посочена информацията по смисъла на чл. 28, ал. 1, т. 4 от Правилника за дейността на Комисията за защита на личните данни и на нейната администрация (ПДКЗЛДНА), т.е. не е посочено лице, срещу което е подадено искането, респ. по същото не може да бъде образувано производство по Раздел II от ПДКЗЛДНА.

Съгласно съображение (97) и разпоредбата на чл. 37, пар. 5 от Регламент (ЕС) 2016/679 администраторът или обработващият лични данни следва да бъде подпомаган при наблюдението на вътрешното спазване на ОРЗД от лице с „експертни познания и професионални качества" в областта на правото и практиките за защита на данните.

Правната уредба, разписана в съображение (97) и разпоредбата на чл. 37, пар. 6 от Регламент (ЕС) 2016/679 определя длъжностното лице по защита на данните, като „служител" или „член на персонала". Граматическото тълкуване на тези понятия показва, че законодателят е имал предвид конкретни физически лица, независимо дали са служители на администратора или обработващия или служители на външна организация, предоставяща услуги в областта на защитата на личните данни.

Разпоредбата на чл. 37, пар. 6 от Регламент (ЕС) 2016/679 допуска възможността ДЛЗД „да изпълнява задачите въз основа на договор за услуги". Логическото тълкуване показва, че ДЛЗД не е задължително да бъде страна по договора за представянето на услугата. Напротив, то винаги следва да е конкретен служител, изпълняващ задачите, произтичащи от договора.

Съгласно разпоредбите на чл. 37, пар. 7, чл. 38, пар. 4, чл. 39, пар. 1, б. д) от Регламент (ЕС) 2016/679 длъжностното лице по защита на данните е точка за контакт за субектите на данни, за служителите на администратора и за надзорния орган. Според Насоките за длъжностните лица по защита на данните („ДЛЗД") на Европейския комитет за защита на данните „целта на тези изисквания е да се гарантира, че субектите на данни (както в рамките на организацията, така и извън нея) и надзорните органи ще могат лесно и пряко да се свързват с ДЛЗД, без да се налага да осъществява контакт с друга част на организацията". Непосредственият контакт с ДЛЗД е особено важен в процедурата по уведомяване на надзорния орган за нарушение на сигурността на личните данни по смисъла на чл. 33 от Регламент (ЕС) 2016/679, предвид краткия 72-часов срок, отреден за предприемане на

действия и комуникация. Това е съществена гаранция за правата на субектите на данни от една страна, а от друга е проявление на спазването на принципа за отчетност, заложен в ОРД.

Съгласно разпоредбата на чл. 38, пар. 3 от Регламент (ЕС) 2016/679 ДЛЗД **„не може да бъде освобождавано от длъжност"**, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Също така администраторите/обработващите лични данни са длъжни да гарантират, че ДЛЗД **„не получава никакви указания във връзка с изпълнението на тези задачи"** и **„се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни"**.

„Според ОРЗД санкционирането е забранено само ако се налага в резултат на изпълнението на задълженията на ДЛЗД в качеството му на ДЛЗД. Например ДЛЗД може да прецени, че дадено обработване би могло да доведе до голям риск и да посъветва администратора или обработващия лични данни да направи оценка на въздействието върху защитата на данните, но администраторът или обработващият лични данни да не е съгласен с оценката на ДЛЗД. В такъв случай ДЛЗД не може да бъде освободено от длъжност поради факта, че е дало този съвет."[1]

С нормите на съображение (97) и чл. 38, пар. 6 от Регламент (ЕС) 2016/679 се очертават характерните особености на длъжността на ДЛЗД – **„да изпълнява своите задължения и задачи независимо"** и функциите му **„да не водят до конфликт на интереси"**, независимо дали ДЛЗД е член на персонала на администратора/обработващия, дали съвместява длъжността или изпълнява задачи по договор за услуги. Направените уточнения налагат ДЛЗД да е лице различно от администратора/обработващия, както и от лицата, които определят целите и средствата за обработването на лични данни при съответния администратор/обработващ (като например управител, главен изпълнителен директор, главен оперативен директор, главен финансов директор, главен медицински директор, ръководител на маркетингов отдел, ръководител на отдел „Човешки ресурси" или ръководител на ИТ отдел, но също така и други функции по-надолу в организационната структура, ако въпросните длъжности или функции са свързани с определяне на целите и средствата за обработване на данните).

Съществен елемент от независимостта на ДЛЗД е, че същото **„се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни"** (чл. 38, пар. 3 от ОРЗД). Тази разпоредба дава ясен сигнал, че когато ДЛЗД е служител на администратора/обработващия, включително когато той е публичен орган, неговата позиция следва да бъде организационно и функционално обособена от другите структурни звена на

[1] Насоки за длъжностните лица по защита на данните („ДЛЗД"), приети на 13 декември 2016 г., последно преразгледани и приети на 5 април 2017 г

организацията. Аналогични примери за длъжности в администрацията, които пряко отчитат своята дейност пред най-висшето ръководно ниво са длъжностите на служител по сигурността на информацията и финансовия контрольор. По правило тези длъжности са на пряко подчинение на ръководителя на съответната организация, т.е. функционално ръководството на тяхната дейност не може да бъде опосредено, чрез структурното им позициониране в рамките на административните звена (дирекции, отдели, сектори). Дори когато ДЛЗД изпълнява тази функция по съвместяване или чрез възлагане към друга заемана длъжност, ДЛЗД подлежи на оценка, извършена от съответния пряк ръководител, който в случая, за да бъде изпълнено условието на ОРЗД, е ръководителят на организацията. Това разбиране напълно съответства на изискванията на чл. 4, ал. 1 от Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация, в който се посочва, че оценяващ е ръководителят, на когото съответният служител е непосредствено подчинен – в случая ДЛЗД трябва да бъде оценявано, като държавен служител, заемащ длъжността ДЛЗД съгласно Класификатора на длъжностите в администрацията пряко от органа по назначаването.

В заключение, може да се обобщи, че ОРЗД осигурява няколко гаранции, с които се дава възможност на ДЛЗД да действа независимо:

- не се дават указания от страна на администраторите или обработващите лични данни по отношение на изпълнението на задачите на ДЛЗД;
- не се допуска освобождаване от длъжност от страна на администратора във връзка с изпълнението на задачите на ДЛЗД;
- не се допуска конфликт на интереси с евентуални други задачи и задължения.

Това обаче не означава, че ДЛЗД е безотчетно, безконтролно и безотговорно пред администратора/обработващия, включително когато е публичен орган. В този смисъл предвиденият в Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация механизъм за оценка на дейността на държавния служител, заемащ длъжността ДЛЗД, не противоречи на изискването за отчетност и независимост по Регламент (ЕС) 2016/679 на ДЛЗД пряко пред най-висшето ръководство на публичния орган. Нещо повече, ОРЗД изисква ДЛЗД да е независимо при изпълнението на възложените му задачи по смисъла чл. 39, като то не носи лична отговорност по ОРЗД, в случай на неспазване на изискванията за защита на данните. Администраторът или обработващият лични данни е този, който е длъжен да гарантира и да бъде в състояние да докаже, че обработването се извършва в съответствие с ОРЗД. Спазването на разпоредбите за защита на данните е отговорност на администратора или обработващия лични данни. В същото време, ДЛЗД може да носи дисциплинарна отговорност по общия ред, например нарушение на

трудовата дисциплина, в случай на кражба, физически, психологически или сексуален тормоз или подобни груби прояви на поведение, несъвместимо с трудовата дисциплина и т.н.

По тези съображения и на основание чл. 58, пар. 3, б. б) от Регламент (ЕС) 2016/679 във вр. с чл. 10а, ал. 1 от Закона за защита на личните данни, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

Предвиденият в Наредбата за условията и реда за оценяване изпълнението на служителите в държавната администрация механизъм за оценка на дейността на държавния служител, заемащ длъжността ДЛЗД, не противоречи на изискването за независимост на ДЛЗД по чл. 38, пар. 3 от Регламент (ЕС) 2016/679.

ПРЕДСЕДАТЕЛ:

ВЕНЦИСЛАВ КАРАДЖОВ /П/

ЧЛЕНОВЕ:

ЦАНКО ЦОЛОВ /П/

МАРИЯ МАТЕВА /П/

ВЕСЕЛИН ЦЕЛКОВ /П/