

Изх. № 26/14.05.2018 г.

ДО

**Г-Н ВЕНЦИСЛАВ КАРАДЖОВ,
ПРЕДСЕДАТЕЛ НА КОМИСИЯТА
ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ**

ОТНОСНО: Проект на Закон за изменение и допълнение на Закона за защита на личните данни

УВАЖАЕМИ ГОСПОДИН КАРАДЖОВ,

Бихме желали да изразим нашата благодарност за възможността да предоставим бележки, коментари и предложения по текста на проекта на Закон за изменение и допълнение на Закона за защита на личните данни („Проектозакон“ и „ЗИДЗЗЛД“). Българската асоциация на управляващите дружества (БАУД) приветства извършената сериозна и качествена работа от страна на ръководителите и експертите от Комисията за защита на личните данни (КЗЛД) за имплементиране на новото европейско законодателство, регулиращо защитата на личните данни и за адаптиране на националното законодателство към изискванията на 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 („Регламента“ и “GDPR”).

Считаме, че се прави важна стъпка в уредбата на дейността по защита на личните данни на гражданите, като приветстваме стремежа на българските държавни органи и администрация да подхождат с мисъл и разбиране за мащабите на дейността на българските юридически лица и особено - на малките и средни предприятия (МСП), когато се транспонират европейски законодателни актове, и да се борят за съразмерност на приеманото законодателство.

Бихме желали да насочим Вашето внимание към някои наши бележки, коментари и предложения по Проектозакон, които ако бъдат отчетени, в още по-голяма степен биха съдействали този всеобхватен нормативен акт да осигури необходимите условия за защита

на личните данни, без обаче предприятията да понасят прекомерни тежести, несъобразени с мащаба на дейността им.

Като обща бележка считаме, че срокът на обществената консултация по проекта на ЗИДЗЗЛД следва да е минимум 30 дни, защото в конкретната хипотеза не е налице изключителен случай. Посоченият в мотивите на ЗИДЗЗЛД аргумент в полза на необходимостта от намаляване на срока на обществената консултация е: "В съответствие с чл. 26, ал. 2 и 4 от Закона за нормативните актове по законопроекта са проведени обществени консултации с гражданите и юридическите лица, като срокът за предложения и становища е намален на 14 дни, предвид обстоятелството, че приближава крайният срок за транспониране на Директива 2016/680/ЕС." Крайният срок за транспониране на Директивата е 4 май 2018 г., но доколкото датата на публикуване на Директива 2016/680/ЕС е 6 май 2016 г., имало е възможност в периода от почти две години да се предприемат необходимите стъпки за транспониране на Директивата. Предвид дългите срокове за влизане в сила на новото европейско законодателство за защита на личните данни, считаме, че не е налице "изключително обстоятелство" по смисъла на чл. 26, ал. 4 ЗНА (форсмажорни обстоятелства като природни бедствия и стихии, военни конфликти и пр.), които биха наложили едно по-кратко по време обсъждане на ЗИДЗЗЛД.

Други конкретни бележки по Проектозакона сме изложили в Приложение № 1 към настоящото писмо.

В заключение, изразяваме нашата готовност да участваме в дискусия и/или работна среща по новото законодателство, уреждащо дейността по защита на личните данни, като изложим допълнителни аргументи в подкрепа на нашите предложения.

С най-сърдечни пожелания за успешна работа!

С уважение:

Петко Кръстев

Председател на УС на БАУД

1. По § 5 и чл. 9, ал. 2

„(2) Комисията урежда в правилник своята дейност, дейността на администрацията си и производствата, които се развиват пред нея, и го обнародва в „Държавен вестник“.“
Предлагаме да отпадне изразът „и производствата, които се развиват пред нея“.

Мотиви: Уредбата на производствата пред нея следва да се уреждат в закона или в наредба, която да действа спрямо трети лица. В правилник за дейността обикновено се уреждат вътрешни отношения, свързани със структурата, организацията и дейността на КЗЛД и нейната администрация. Обжалване на правилника като вид административен акт може да блокира дейността на КЗЛД, докато атакуването на наредба, която урежда отношения свързани с прилагането на закона, няма да има такъв блокиращ дейността на цялата институция ефект.

2. По §6 и чл. 10, ал. 2

Точки 11 и 14 се дублират. Следва в една точка да се уреждат правомощията на КЗЛД да издава подзаконови нормативни актове. Навсякъде в този член следва да се постановява, че КЗЛД издава актове от нейната (специална) компетентност не общо в областта на защита на личните данни, а на законово/нормативно основание, при законова делегация, т.е по прилагане на нормативните актове като ЗЗЛД и GDPR. Народното събрание е органът, който може първично да урежда отношения, касаещи защитата на личните данни, поради важността на материята и правата, които може да бъдат засегнати - с актове съгласно Конституцията – закони.

3. По §9 и чл. 12, ал. 3 и §19 и чл. 38, ал. 1

Предлагаме сроковете по двата текста да се редуцират, макар и по различни съображения.

Мотиви: Срокът от 8 и съответно 6 седмици по чл. 12, ал. 3 при даване на становища от КЗЛД на администратори на лични данни при предварителни консултации следва да се намалят. Нуждата от по-голяма оперативност и яснота относно дейността на администраторите на лични данни, когато се изисква оценка на рисковете, налага това да става в кратки времеви граници, за да не се създава правна несигурност и потенциал за нарушаване на правата на лицата, чиито лични данни са обект на защита.

Що се отнася до чл. 38, ал. 1, той в Проектозакона гласи:

„(1) При нарушаване на правата му по Регламент (ЕС) 2016/679 и този закон всеки субект на лични данни има право да сезира комисията в едногодишен срок от узнаване на нарушението, но не по-късно от пет години от извършването му.“

Считаме, че лицата следва своевременно да предявяват претенции и жалби и когато реално са били нарушени правата им. Прекалено дългите срокове за реакция при предполагаемо нарушение на права, свързани със защитата на лични данни, са необосновани, доколкото ако е изминал дълъг срок, през който не са предприети действия и не са се проявили ефекти и последици от нарушението, най-вероятно означават, че или не е имало нарушение или то понекакъв начин не е засегнало правната сфера на правоимащите лица. Следва да ес отчита и обсъждателството, че една немалка част от

личните данни се съхраняват за доста по-кратки срокове, което ще направи трудно или невъзможно защитата на предприятията, спрямо които са предявени претенции.

Освен това, предлагаме навсякъде седмичните срокове да се преизчислят в дни и/или месеци, доколкото това е разпространената в България практика при броене на срокове и по този начин се процедира в повечето законови актове, в които се предвижда определяне на срокове за извършване на определени действия.

4. По § 12 (нов чл. 15, ал. 2)

Чл. 15, ал. 2 гласи:

...

(2) Обучението по ал.1, когато е по искане на администраторите, обработващите или обучаващите се, е за тяхна сметка и се заплаща по тарифа, определена от министъра на финансите.“

Според нас позициите в тарифата следва да бъдат уредени на законово ниво като основание и да се делегира на Министерството на финансите или на Министерския съвет (с оглед да не се правят чести, конюнктурни и неоправдани изменения в нея) да приема тарифа. Това може да се уреди и на ниво закон по същите съображения и *per argumentum a fortiori*.

Съответно, за обученията по инициатива на КЗЛД, като една от вменените задачи и функции на Комисията по чл. 79, ал. 1, т. 4, за които не се дължат такси, е желателно е да се предвиди обученията по чл. 79, ал. 1, т. 4 да се провеждат на определена минимална честота за определени сектори (напр. финансовия), включително и с използване на технически средства за дистанционно обучение.

5. По § 15 и нов чл. 25б, ал. 1 и 3

А) Чл. 25б. (1) Извън случаите по чл. 37, пар. 1 от Регламент (ЕС) 2016/679 администраторът или обработващият лични данни задължително определя длъжностно лице по защита на данните, когато обработва лични данни на над 10 000 физически лица.

Предлагаме този текст да отпадне, доколкото не се съдържа в GDPR и представлява случай на *gold plating*, т.е. въвеждане на по-тежки и рестриктивни изисквания, отколкото заложените в европейското законодателство.

Мотиви: При всички случаи, цифрата 10 000 е произволно заложена, не се основава на предварителни оценки и статистика, като минимум следва да бъде увеличена, на базата на проведени проучвания и анализ, както и да се добави уточнение, че изискването не се прилага ако личните данни са единствено е-мейл адреси за целите на кореспонденцията, тъй като това представлява нисък риск за правата и свободите на лицата и не предполага мащабна и регулярна обработка.

Българското законодателство не следва да бъде по-рестриктивно от европейската рамка за дейността на администраторите и обработващите лични данни. Текстът може да се редактира, като се остави възможност по преценка на администратора/обработващия данните да се назначи длъжностно лице по защита на данните (ДЛЗД). Не следва да се допуска разширяването на основаната на Регламента уредба (макар той да допуска това). Хипотезата на чл. 37(1)(б) от GDPR може да се специфицира с число (10 000 все пак е малко), но да се запази изискването обработката да бъде редовна и мащабна. В противен случай в оценката на въздействието трябва да се включи цената на наетите/преназначените/обучените длъжностни лица по защита на данните. Тези аргументи в още по-голяма сила важат за микропредприятията и МСП.

Б) Чл. 25б, ал. 3

„(3) Длъжностното лице по защита на данните може да изпълнява задачите си по трудово или служебно правоотношение, вкл. по вътрешно съвместителство, или въз основа на договор за услуги. Администраторът и обработващият не могат да съвместяват и функциите на длъжностно лице по защита на данните.“

Администраторът и обработващият не са длъжни да назначават ДЛЗД. Това означава, че тези функции следва да се поемат от администратора/обработващия (ако той е ФЛ) и от негови служители или определени от него лица (ако е ЮЛ), които изпълняват функции, свързани със защитата на лични данни. Тексът следва да се поясни, защото прилагането на текста в този му вид ще означава, че във всички случаи всяко лице, независимо дали са налице предпоставките за това и съответен обхват и размер на дейността, ще трябва да назначава ДЛЗД.

В) По чл. 25д

„Чл. 25д. (1) Когато при упражняването на правото на свобода на изразяване и информация, включително за журналистически цели и за целите на академичното, художественото или литературното изразяване, се обработват лични данни на физически лица, администраторът на лични данни прави преценка за законосъобразността на обработването във всеки конкретен случай. Решението на администратора не може непропорционално да ограничава свободата на изразяване и информация.“

Предлагаме уточняване дали понятието „академични цели“ включва в съдържанието си и обучения и образователни курсове, които се организират от професионални и браншови организации, подготвят кадри в своята специализирана област, извън академични и научни заведения. Ако се възприеме тясно тълкуване, е възможно да се ограничи и затрудни дейността по повишаване квалификацията на експерти от съответните области.

6. По § 22 и чл. 47, т. 2 – предлагаме да се уточни, че текстът касае лица, осъдени за престъпления, **с влязла в сила присъда** (освен ако не се разграничават случаите на осъдени, но по висящи производства и такива, за които има влязла в сила осъдителна присъда).

7. По § 22. Разпоредбата на чл. 62, ал. 1 от законопроекта вменява задължение за всеки администратор да поддържа регистър с всички категории дейности по обработване /респ. ал. 2 - за обработващите/. Тази разпоредба противоречи на чл. 1, ал. 6 от проектозакона, както и на духа и смисъла на GDPR според които политиката за защита на лични данни следва да отчита **специалните потребности на микропредприятията, малките и средни предприятия**. Именно поради тази причина съображение (13) от Регламента въвежда дерогация за организации с по-малко от 250 служители по отношение на воденото на регистър. Тази дерогация следва да бъде отразена и в законопроекта.

8. По §23 и чл. 84, ал. 2

„(2) Мерките по ал. 1 се издават по ред и условия, определени в Правилника за дейността на комисията.“

В закона следва да се уредят принудителните административни мерки, които КЗЛД може да налага. Това произтича от принципа на законност, пропорционалност, справедливост и обоснованост на ПАМ, които се налагат. Не следва на подзаконово ниво да се уреждат мерки, които могат да създават условия за административен произвол и налагане на ПАМ, които е невъзможно да бъдат изпълнявани от адресатите на правните норми. В закона следва да се уредят възможните ПАМ, които да са *numerus clausus*, като се представи възможност на субектите на правото да организират дейността си по начин, който да им позволява да я съобразяват с изискванията на закона и възможните последици от неговото нарушаване.

9. По чл. 85

„Чл. 85. (1) За нарушения, посочени в чл. 83, параграф 5 и параграф 6 от Регламент (ЕС) 2016/679 и за нарушения на чл. 45, ал. 1, чл. 49, ал. 1, чл. 52, чл. 54-56, чл. 80, ал. 1, т. 1, б. „а“, т. 2, б. „б“ и б. „в“ от глава осма администраторът или обработващият лични данни се наказва с глоба или имуществена санкция от 10 000 до левовата равностойност на 20 000 000 евро.

(2) За нарушения по чл. 83, параграф 4 от Регламент (ЕС) 2016/679, чл. 59, чл. 62, чл. 64-69 от глава осма административното наказание глоба или имуществена санкция е в размер от 5000 до левовата равностойност на 10 000 000 евро.

(3) За други нарушения по този закон администраторите и/или обработващите лични данни се наказват с глоба или с имуществена санкция от 1000 до 5000 лв.“

Считаме, че следва радикално да се намалят минималните размери на санкциите.

Мотиви: Прекалено високият максимален размер, който произтича директно от GDPR, е въведен с предупредителна и превантивна цел, съобразен е с нивото на икономическото развитие на водещите в стопанско отношение държави, но тези размери не съответстват на икономическите стандарти в малките и догонващи по-напредналите в своето развитие държави-членки на Европейския съюз.

Същата бележка може да се направи и по отношение на високия размер на санкциите за неизпълнение на принудителна административна мярка (ПАМ) по чл. 88 (от 2000 до 200 000 лв.), като такъв размер може да се прилага само ако не е изпълнена **влязла в сила ПАМ**. Същото се отнася и до размера на наказанията по чл. 90 („Чл. 90. За други нарушения по Регламент (ЕС) 2016/679 се издава задължително предписание или се налага административно наказание глоба или имуществена санкция в размер от 2 000 лв. до 200 000 лв. по реда и условия, определени в чл. 84 и чл. 87.“).

Защо е необходимо да се избегне значителното увеличаване на санкциите за нарушаване на **ЗЗЛД и Регламента** и по-точно – **на техните минимални размери**? В европейското законодателство се уреждат „минимални“ максимални прагове на глобите, но европейският законодател оставя на националните регулатори да установят минималните прагове, именно поради необходимост да се спази принципът на пропорционалността, да се отчете националната специфика и размерите, ниво на развитие и икономическите стандарти на отделните държавни-членки на Европейския съюз. В практиката изобилстват случаи на формални нарушения или нарушения без вредоносен резултат и без да се създават заплахи за нормалното функциониране на системата от отношения по защита на личните данни. По отношение на такъв тип нарушения не е

целесъобразно да се налага завишени по размер санкции, като следва на правоприлагащите органи да се предостави възможност да отчитат в по-голяма степен характера и тежестта на нарушенията. В последните години няма и фундаментална промяна в параметрите на икономиката, които да оправдават увеличаване на минималните размери на санкциите.

В тази връзка, предлагаме сериозно количествено редуциране на минималните размери на санкциите по ЗЗЛД, но не по-малко от два пъти спрямо предложените нива.

10. По чл. 87, ал. 5 – считаме, че глобите и имуществените санкции следва да не постъпват в бюджета на КЗЛД, а в централния държавен бюджет.

В тази връзка предлагаме следната редакция на текста:

„Чл. 87, ал 5. Глобите и имуществените санкции, наложени от комисията, се внасят в държавния бюджет по сметка на Националната агенция за приходите.”

Мотиви: считаме, че събраните суми от наложени имуществени санкции следва да се насочват към държавния бюджет, за да се избегнат фискалните съображения при налагането на най-тежките имуществени санкции и глоби и да се постави фокуса върху превенцията, с цел постигане на целите на закона и висока степен на обществено доверие в законността и справедливостта на налаганите санкции. По подобен начин са уредени отношенията, свързани със събирането на глоби и имуществени санкции в Закона за Комисията за финансов надзор, който може да послужи за модел за уреждане на тази материя, доколкото създава условия и гаранции за избягване на конфликти на интереси и самоцелно налагане на глоби, без да има възможност постъпленията от глоби и санкции да се използват за материално стимулиране на администрацията.

11. По чл. 89, ал. 2

„(2) Административните наказания и/или принудителните административни мерки по Регламент (ЕС) 2016/679 по ал. 1 се налагат с решение на комисията по ред и условия, определени в Правилника за дейността на комисията.“

Административните наказания следва да се налагат по реда на ЗАНН или въз основа на специални правила, разписани на законово ниво, ако ЗАНН (съответно НПК) се прилагат субсидиарно.