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

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
Регистрационен индекс и дата
НДМСПО-01-697#..3...../15.10.2018 г.

ДО
Г-Н ХРИСТО ХРИСТОВ
ПРЕДСЕДАТЕЛ НА УПРАВИТЕЛНИЯ СЪВЕТ НА
СДРУЖЕНИЕ „ИНТЕРАКТИВ АДВЪРТАЙЗИНГ БЮРО БЪЛГАРИЯ“

ГР. СОФИЯ
УЛ. „НАЙДЕН ГЕРОВ" № 6, ЕТ. 4,
ОФИС 7

ОТНОСНО: Проект на „Секторен кодекс за защита на личните данни в дигиталния сектор“

УВАЖАЕМИ ГОСПОДИН ХРИСТОВ,

Приложено, изпращаме Ви становище на Комисията за защита на личните данни, изразено на основание чл. 58, пар. 3, буква „г" от Регламент (ЕС) 2016/679 (Общ регламент за защита на данните), във връзка с Ваше искане с вх. № НДМСПО-01-697/27.06.2018 г. за одобрение на проект на Кодекс за поведение.

ПРИЛОЖЕНИЕ: Съгласно текста

ПРЕДСЕДАТЕЛ:
Венцислав Караджов

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

СТАНОВИЩЕ

НА

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

рег. № НДМСПО-01-697/27.06.2018 г.

гр. София, 15.10.18

ОТНОСНО: Искане за одобрение на проект на **„Секторен кодекс за защита на личните данни в дигиталния сектор"**

Комисията за защита на личните данни (КЗЛД) в състав - членове: Цветелин Софрониев, Мария Матева и Веселин Целков, на заседание, проведено на 19.09.2018 г., разгледа искане с вх. № НДМСПО-01-697/27.06.2018 г. от Христо Георгиев Христов, Председател на УС на сдружение „Интерактив Адвъртайзинг Бюро България", за одобрение на проект на „Секторен кодекс за защита на личните данни в дигиталния сектор".

Кодексът е подаден на основание чл. 40 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Регламент). Предложеният за одобрение Кодекс съдържа 36 страници. Съдържанието му е разделено на **девет раздела**, както следва:

Раздел I. Съгласие за обработка на лични данни.
Раздел II. Събиране на лични данни.
Раздел III. Оттегляне на съгласието за обработка на лични данни.
Раздел IV. Информация, предоставяна от Администратора на субекта на данните.
Раздел V. Упражняване на правата от субектите на данните по GDPR.
Раздел VI. Съответствие с GDPR на администратори на лични данни.
Раздел VII. Обработващ на личните данни.
Раздел VIII. Задължено лице по Кодекса.
Раздел IX. Сигурност и съответствие с GDPR при обработването на лични данни.

Към Кодекса са предоставени **шест броя приложения**.

Кодексът за поведение по смисъла на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. е доброволен инструмент, който има за цел да улесни ефективното прилагане на Регламента, както и да спомогне за доказването на факта на спазване на нормативните изисквания в съответствие с принципа за отчетност, като се отчитат особеностите на обработването на данни в определени сектори или професии.

Разработването и приемането на Кодекс за поведение не е задължително изискване и е въпрос на преценка на сдружението или друга структура, представляваща съответната категория администратори или обработващи лични данни.

Кодекс за поведение се изготвя за отделна категория администратори/обработващи лични данни (АЛД/ОЛД), по-специално ако същите принадлежат към един и същи сектор или бранш.

Кодексът за поведение има добавена стойност само тогава, когато е изготвен специално за конкретен сектор или бранш, отразява неговите особености и съществуващите практики при обработването на лични данни, като например специфичните рискове за правата и свободите на субектите на данните и подходящите технически и организационни мерки за тяхното ограничаване. Това логично означава, че съответният сектор, бранш или категория администратори/обработващи лични данни следва да имат достатъчно добро ниво на самоорганизираност и ефективни механизми за вътрешна координация и контрол.

Инициативата за изготвяне на Кодекс за поведение следва да произлиза от съответния сектор или бранш. Когато изготвят, изменят или допълват Кодекс за поведение, сдруженията (асоциациите, камарите) и другите структури, представляващи категорията АЛД/ОЛД, следва да се консултират със съответните заинтересовани страни, включително със субектите на данни (публична консултация), когато това е осъществимо, и да вземат под внимание становищата, изразени писмено и устно в рамките на тези консултации.

Кодексите за поведение следва да са написани на достъпен и разбираем език и да отчитат националните особености и практики.

Всеки Кодекс следва да е съобразен с разпоредбата на чл. 40 от Регламент (ЕС) 2016/679 относно защитата на данните, която дава правната рамка по отношение съдържанието му. В Кодекса следва да бъде уточнено приложението на изискванията на Регламента в конкретния сектор/бранш/отрасъл. Затова е недопустимо използването на декларативни изявления, без същите да представят подходящи гаранции за правата и свободите на субектите на данни при обработването на техни лични данни, както и преписването (копирането) на текстове от Регламента

Независимо от прякото действие на Регламента, с цел създаване на улеснение при изготвянето на Кодексите за поведение, КЗЛД прие критерии и процедури по одобряване на Кодекси за поведение. Целта на приетите критерии и процедури е да уточнят някои параметри на Регламента, за да се подпомогне еднаквото разбиране и прилагане на неговите изисквания при изготвяне на Кодекси за поведение.

Критериите за одобряване на Кодекс за поведение имат за цел извършване на оценка дали и доколко Кодексът за поведение отговаря на чл. 40 от Регламент 2016/679. Ако някоя от хипотезите на чл. 40 не е приложима, трябва да бъде предоставена информация за това.

Анализ:

При разглеждането на предложения от Сдружение „Интерактив Адвъртайзинг Бюро България“ **СЕКТОРЕН КОДЕКС ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ДИГИТАЛНИЯ СЕКТОР**, съобразно изискванията по чл. 40 от Регламент 2016(679) и на критериите на Комисия за защита на личните данни и направения обстоен анализ, се установи следното:

1. Да са посочени предметът и обхватът на Кодекса.

В Кодекса са посочени предметът и обхватът, както и кой го предлага. Предоставена е обща информация за представителността – участници от дигиталния сектор.

Разнородната дейност, която изпълняват членовете на сдружението, които се предвижда да прилагат проекта на Кодекса, обаче поставя сериозно под съмнение, дали поначало Кодекса по чл. 40 от Регламента може да бъде приложим в конкретния случай.

Разнородният характер на администраторите е пречка за уточняване приложението на Регламента в цялост, по отношение на конкретен сектор.

Видно от предложения Кодекс, единствената обща характеристика между всички администратори е обработването на лични данни в дигитална среда, което е само част от дейностите по обработване.

Подобен фрагментарен подход не само поставя под въпрос добавената стойност на предложеният Кодекс, но и не улеснява АЛД при обработването на данни, свързано с основният им предмет на дейност, респективно не гарантира изпълнението в цялост на задълженията по Регламента.

2. Да съдържа критерии за присъединяване на АЛД/ОЛД към Кодекса.

Посочено е кой може да се присъединява към този Кодекс (Задължени лица по кодекса – чл. 18), а именно:

- Юридическо лице, което предлага услуги, свързани с дигиталния сектор и което е изразило съгласието си да се придържа към изискванията на този Кодекс.
- Юридическо лице, което е член на ИАБ България и се е задължило пред ИАБ България да се съобразява с изискванията на този Кодекс.

Въпреки че са дефинирани задължените лица по Кодекса, отново остава спорен въпросът за принадлежността им в общ сектор.

3. Да съдържа описание на механизма за присъединяване към Кодекса и обвързващата сила на това присъединяване. Да съдържа описание на механизма за прекратяване или временно спиране на присъединяването към Кодекса.

Предложеният проект на Кодекс не съдържа описание на механизма за присъединяване към Кодекса и обвързващата сила на това присъединяване, както и описание на механизма за прекратяване или временно спиране на присъединяването към Кодекса.

4. Да съдържа описание на механизмите за извършване на задължително наблюдение за спазването на неговите разпоредби от АЛД/ОЛД, които приемат да го прилагат. Тези механизми не трябва да засягат задълженията и правомощията на надзорните органи.

Предложеният проект на Кодекс за поведение не съдържа описание на механизмите за извършване на задължително наблюдение за спазването на неговите разпоредби от АЛД/ОЛД, които приемат да го прилагат.

5. Да съдържа общи критерии и механизми за извършване на анализ на риска и ако е приложимо – общи изисквания към извършване на оценка на въздействието по чл. 35 от Регламента.

Предложеният проект на Кодекс не съдържа критерии и механизми за извършване анализ на риска, поради което не може да се направят изводи доколко се гарантира сигурността на обработването.

Оценката на въздействието върху защитата на данните е представена общо, без да се отчитат особеностите и спецификите, присъщи на сектора. В чл. 22, ал. 4 са изброени операции с лични данни, за които не се изисква извършване на оценка на въздействието на защитата на личните данни, за което не са представени нито аргументи, нито методология, на която се обосновава този извод.

6. Да съдържа описание на механизмите за подпомагане отчетността чрез предоставяне на образци на документи.

Приложени са образци на документи, които са свързани преди всичко с даване и оттегляне на съгласие за обработка, искане за изтриване и искане за преносимост на лични данни от субектите на данни.

Не са представени образци на документи и документация по анализ на риска и оценка на въздействието, вътрешни правила, технически и организационни мерки.

В тази връзка не може да се направи обоснован извод за изпълнение на принципа за отчетност.

7. Да има описание на категориите лични данни и/или регистрите, съдържащи лични данни, които обработват АЛД/ОЛД, присъединили се към Кодекса– какви данни се събират, за какви цели, срок за съхранение, срок за задържане и т.н.

Описани са категориите лични данни, които администраторът събира от субекта на данните за доставка на стоки чрез договор, сключван от разстояние, и за изпълнение на договор за възмездна услуга. Не са посочени конкретни срокове за съхранение на данните.

Поради разнородната дейност на администраторите, предвидени да прилагат Кодекса, направеното описание на категориите данни ограничава добавената стойност на тази информация за АЛД, т. к. множество други операции по обработване остават извън обхвата на Кодекса.

8. Да е посочено как се събират, обработват и съхраняват личните данни, включително и правното основание.

Липсва описание на технологията на обработване лични данни и потоците информация, съдържащи лични данни. Не е посочено как се събират обработват и съхраняват личните данни. В Кодекса липсва ясно разграничение на дейностите по обработване на данни, регистрите с лични данни, за които се отнасят, както и приложимото за всяко едно от тях правно основание.

По отношение приложимостта на съгласието като правно основание, следва да се отчита и обстоятелството, че събирането и обработването на лични данни в по-голям обем от нормативно предвидения, би могло да доведе до нарушение на принципите за „законосъобразност“ и „свеждане на данните до минимум“ (арг. чл. 5, б. „а“ и „в“ от

Регламента). В тази връзка обработването на ЕГН на основание съгласие е в нарушение на горепосочените принципи.

Не е отразено как се изпълняват задълженията на администратора по чл. 30 от Регламента.

9. Да са посочени законните интереси на АЛД/ОЛД, когато това е приложимо.

В проекта на Кодекс за поведение на няколко места са споменати легитимните интереси на администраторите и обработващите лични данни, присъединили се към Кодекса, но не са определени и конкретизирани. Регламентът допуска обработване на лични данни на това правно основание, само ако легитимните интереси на АДЛ/ОЛД имат преимущество пред интересите или основните права и свободи на субекта на данни. Липсва анализ за наличие на такова преимущество и критериите, по които е достигнато до този извод.

10. Как се гарантира добросъвестно и прозрачно обработване на лични данни. Информиране на обществеността и субектите на данни относно присъединяването към кодекса. Информиране на обществеността и субектите на данни относно правата им по Регламента.

Представен е механизъм за упражняване правата на субектите на данните по Регламента, включително са приложени примерни форми.

В чл. 24 е предвидено Задължените по Кодекса лица задължително да поставят знак за съответствие с изискванията на Кодекса и линк към него. Предвиждат се изисквания към знака, неговото изобразяване и поставяне да бъдат приети от Управителния съвет на ИАБ България.

В раздел IV е представено каква информация предоставя АЛД на субекта на данните, включително и начините/способите на нейното предоставяне. Един от способите, посочен в чл. 10, ал. 2, т. „с“) е „Privacy notice“. В тази връзка, в „Приложение № 5 - Изявление за поверителност (Privacy notice)“ е представена примерна форма. Следва да се отбележи, че терминът „поверителност“ внася терминологична неяснота поради противоречие с неговото значение в Регламента, както и със съдържателната част на Приложение № 5.

При информирането на субектите на данни не става ясно на какво основание се събират обработват и съхраняват различните категории личните данни, тъй като в Кодекса са изброени всички условия за законосъобразност на обработването, съгласно чл. 6, пар. 1 от Регламента (Приложение № 5, чл. 1).

Приложеният образец - „Изявление за поверителност (Privacy notice)“ не улеснява приложението на Регламента т. к. не унифицира приложението на чл. 12 и сл., а само посочва техните реквизити.

11. Какви мерки се предвиждат относно упражняване правата на субектите на данни. Да са посочени категориите лица (физически и юридически), които имат право на

достъп до информацията от регистрите с лични данни, както и степента на този достъп (пълен, ограничен).

В раздел III е разписана процедура за оттегляне на съгласието за обработка на лични данни. В Приложение № 2 е представена примерна форма.

В раздел V - „Упражняване на правата от субектите на данните по GDPR“ са налични процедури относно „Право на корекция на личните данни“, „Право на изтриване („право да бъдеш забравен")“ и „Право на преносимост на данните“. Приложени са примерни форми: „Искане „да бъда забравен" - за изтриване на личните данни, свързани с мен“ (Приложение № 3) и „Искане за преносимост на лични данни“ (Приложение № 4).

Не са посочени категориите лица (физически и юридически), които имат право на достъп до информацията от регистрите с лични данни, както и степента на този достъп (пълен, ограничен).

Не са представени вътрешни регламентиращи документи.

12. Процедура относно информирането и закрилата на децата и начин на получаване на съгласие от носещите родителска отговорност за детето.

В Раздел I, чл. 2 е разписан механизъм за потвърждение на съгласие при събиране на лични данни от физически лица под 16 годишна възраст. В Приложение № 1- „Примерни форми за изразяване на съгласие за целите на обработка“ е налична „Форма за даване на съгласие за обработване на лични данни, предоставени от лице под 16 години“ .

13.Технически и организационни мерки за защита. Да са посочени условията за прилагане на псевдонимизация на данните, ако е приложимо.

Няма дефинирани нива на защита на данните.

Не са посочени технически и организационни мерки за защита, както и доколко е приложима псевдонимизация на данните, с оглед да се гарантира сигурността на обработването.

14. Ако е приложимо – дали и защо Кодексът се явява подходяща гаранция по смисъла на чл. 46, пар. 2, буква д) (предаване на лични данни на трети държави или международни организации).

Налице е пряко противоречие между разпоредбите на чл. 16 и чл. 17 от Приложение № 5 „Изявление за поверителност (Privacy notice)“ поради което не може да се направи категоричен извод дали Кодексът се явява инструмент за трансфер на данни.

15. Процедура за уведомяването на надзорните органи за нарушения на сигурността на личните данни и процедура за уведомяването/съобщаването за такива нарушения на засегнатите субекти на данни.

Не е разписана процедура по приложението на задълженията на администратора по чл. 33 и чл. 34 от Регламента, а единствено е възпроизведено тяхното съдържание.

16. Описание на извънсъдебните производства и други процедури за разрешаване на спорове между администраторите и субектите на данни по отношение на обработването, без да се засягат правата на субектите на данни за подаване на жалба до надзорен орган или ефективна съдебна защита срещу надзорен орган или право на ефективна съдебна защита срещу АЛД/ОЛД.

Не са предвидени извънсъдебни производства и/или други процедури за разрешаване на спорове между администраторите и субектите на данни, а единствено частично са възпроизведени разпоредбите от Регламента, свързани със средствата за правна защита.

Въпреки че е предвидена възможността споровете да се уреждат на доброволна основа чрез преговори, не е уточнен механизмът за това.

17. Да е предвидена процедура за изменението и допълнение на кодекса на поведение.

Не е предвидена процедура за изменение и допълнение на Кодекса за поведение.

18. Процедура за предприемане на съответните действия в случай на нарушение на кодекса от страна на администратор или обработващ лични данни, включително като суспендира членството в кодекса или изключва от него съответния администратор или обработващ лични данни.

Не е разписана процедура за предприемане съответни действия в случай на нарушение на Кодекса от страна на администратор или обработващ лични данни, включително като се суспендира членството в Кодекса или се изключва от него съответният администратор или обработващ лични данни.

Допълнителни бележки:

1. Когато се изготвя, изменя или допълва Кодекс за поведение, сдруженията и другите структури, представляващи категории администратори или обработващи лични данни, следва да се консултират със съответните заинтересовани страни, включително субектите на данни, когато това е осъществимо, и да вземат под внимание становищата, изразени писмено и устно в рамките на тези консултации (арг. съобр. 99 от Регламента). В конкретния случай липсват информация и доказателства за изпълнение на тази процедура.

2. Кодексът следва да съдържа информация дали дейностите по обработване имат отношение към няколко държави членки. В случай, че това е така, е необходимо да бъде представена информация за цялостната технология на обработване.

3. Липсва конкретика, относно начина на приложение на принципите за обработване на лични данни в конкретния сектор/бранш.

4. Използваната в Кодекса терминология следва да съответства на тази в Регламента без да я допълва или изменя.

5. Не е посочена информация за референтност на приложенията към съдържателната част на проекта на Кодекс.

6. Така дефинираният „дигитален сектор“, не допринася присъединилите се към Кодекса администратори и обработващи лични данни да изпълняват изцяло задълженията си по Регламента, с оглед на всички процеси по обработване на данни, произтичащи от предметната им на дейност. Затова следва да се уточни и аргументира доколко визираните в

проекта на Кодекс предмет и обхват са релевантни към посочения сектор, както и критериите по които е дефинирано понятието „сектор“ в конкретния случай, с цел преценка приложимостта на чл. 40 от Регламента.

Във връзка с гореизложеното предложеният Кодекс за поведение съдържа пропуски, които следва да бъдат отстранени, преди да бъде предложен за одобряване.

С оглед на горепосоченото и на основание чл. 58, пар. 3, буква „г" от Регламент (ЕС) 2016/679, Комисията за защита на личните данни изразява следното

СТАНОВИЩЕ:

1. На основание чл. 58, параграф 3, буква „г“ от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета, представения проект на Кодекс за поведение не съответства на Регламент (ЕС) 2016/679, поради което не осигурява достатъчно подходящи гаранции за правата и свободите на субектите на данни.

2. Връща проекта на Кодекс за поведение на вносителя за привеждането му в съответствие с изискванията на Регламент (ЕС) 2016/679.

ЧЛЕНОВЕ:

Цветелин Софрониев

Мария Матева

Веселин Целков