Разяснения относно практическото приложение на Общия регламент за защита на данните от органите на местното самоуправление (общините)

Във връзка с постъпили въпроси относно практическото приложение на Общия регламент за защита на данните от органите на местното самоуправление (общините), КЗЛД дава следните разяснения:

1. **Предвижда ли се да се разработят унифицирани документи или система от документи по защита на личните данни за всички общини или всяка община ще ги разработва поотделно.**

Съгласно съображение 82 от Регламента, за да докаже спазването му, администраторът или обработващият лични данни следва да поддържа документация за дейностите по обработване, за които той е отговорен. В чл. 30 е визирано задължението на администратора да поддържа регистър на дейностите по обработване, като подробно са посочени и реквизитите, които трябва да съдържа. Следва да се отбележи и фактът, че общините са от типа администратори, които обработват лични данни, видът на които, целите и средствата за обработване се определят със специални закони. С оглед възможностите и спецификите на всяка община, разработването на документната система следва да се извърши след анализ и собствена преценка.

2. **Какви са задължителните политики, процедури или други документи, които следва да се разработят и внедрят в общината. Регламентът задължава администраторите да опишат всеки един процес в детайл, а не само като минимални мерки за защита при обработка на данните. Означава ли това, че трябва да бъдат описани всички административни услуги, които общината изпълнява.**

Като се вземе предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира, и да е в състояние да докаже, че обработването се извършва в съответствие Регламента, като тези мерки се преразглеждат и при необходимост се актуализират. Когато това е пропорционално на дейностите по обработване, мерките следва да включват прилагане от страна на администратора на подходящи политики за защита на данните. Следва да се отбележи, че придържането към одобрени кодекси за поведение

или механизми за сертифициране, може да се използва като елемент за доказване на спазването на задълженията на администратора /арг. чл. 24 от Регламента/.

Както вече беше посочено по-горе, в чл. 30 е визирано задължението на администратора да поддържа регистър на дейностите по обработване, като подробно са посочени и реквизитите, които трябва да съдържа. Обръщаме внимание, че администраторът носи отговорност и трябва да е в състояние да докаже спазването на принципите за обработване на лични данни – т. нар. „отчетност“ /арг. чл. 5 от Регламента/.

3. **Очаква ли се да се приемат общи национални правила по защита на личните данни (Кодекси за поведение) и кога евентуално.**

Съгласно чл. 40 от Регламента изготвянето на кодекс за поведение е правна възможност, т.е. не е задължително. Той може да се изготвя от администраторите/обработващите лични данни, като целта му е да се улесни ефективното прилагане на Регламента, като се вземат предвид особеностите на обработването на данни в определени сектори и специфичните потребности на администраторите/обработващите. В този ред на мисли, добра практика е кодексите да се изготвят на отраслово (браншово) ниво. В тях може да се установят параметрите на задълженията на администраторите и обработващите лични данни, като се вземе предвид рискът, който е вероятно да произтече от обработването на данни за правата и свободите на физическите лица. Проектът на кодекс, негово изменение или допълнение, следва да се предостави на надзорния орган, който е компетентен да се произнесе със становище дали съответства на Регламента и го одобрява, ако установи, че осигурява достатъчно подходящи гаранции.

4. **За общините задължително ли е назначаването на длъжностно лице по защита на данните.**

В чл. 37, пара. 1 от Регламента се предвижда длъжностно лице по защита на личните данни да се определя задължително от:

- Публични органи или структури, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;

- Администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и систематично мащабно наблюдение на субектите на данни;

- Администратори, чиито основни дейности се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

Във връзка с посоченото, общините попадат в категорията на публичните структури и са задължени да определят длъжностно лице по защита на данните.

5. **Какви са правните възможности за уреждане на взаимоотношенията между администратора на лични данни и длъжностното лице по защита на данните (DPO) – трудов договор, граждански договор или със заповед да се възложат допълнително функции на служител от администрацията, който да съвместява две длъжности, като се допише длъжностната му характеристика.**

Лицето по защита на личните данни може да бъде част от персонала, но може и да е външен субект, който изпълнява своите задължения въз основа на сключен граждански договор. Затова администраторите нямат задължение да назначават специално такъв служител, а само имат задължение да определят лице, което да изпълнява функциите на служител но защита на данните.

Няма пречка служителят, определен за лице по защита на данните, да изпълнява и други функции в рамките на организацията, но те не следва да водят до конфликт на интереси. Изборът на вид правоотношение, при които се определя или назначава лице по защита на личните данни, е изцяло в преценката на администратора на лични данни.

6. **Кога личните данни се обработват законосъобразно на основание „изпълнението на задача от обществен интерес“.**

Обръщаме Ви внимание, че понятието „обществен интерес“ се използва в смисъла на едно от алтернативните основания за законосъобразност на обработване на лични данни съгласно чл. 6 от Регламента. Във връзка с качеството си на публичноправен субект в голямата част от своята дейност, общината обработва лични данни на основание спазване на законово задължение за администратора.

Понятието „обществен интерес“ е изключително трудно, а вероятно и невъзможно за дефиниране, като се държи сметка за обстоятелството, че става дума за абстрактна правна, политологическа, философска и социално-икономическа категория, чието съдържание зависи не само от състоянието на обществото в конкретен исторически момент, но и от индивидуалните интереси на членовете на обществото.

Обществениият интерес не може и не трябва да бъде дефиниран, тъй като той винаги ще се влияе от време, място и възгледи.

Легална дефиниция за обществен интерес няма, макар че масово се използва понятието в редица нормативните актове. Извеждането на обществения интерес е въпрос на тълкуване за всеки конкретен случай.

7. **Трябва ли да се изчака да се приемат промените в законовите и подзаконовите нормативни актове, които ще дадат по-голяма конкретика или да се започне работа от общината по привеждането на политиките и процедурите в съответствие с Регламента.**

От 25 май 2018 г. във всички държави-членки на ЕС започва прякото прилагане на Общия регламент за защита на данните /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/. Регламентът бе обнародван в Официален вестник на Европейския съюз на 04.05.2016 г., а отложеното му прилагане бе продиктувано от необходимостта бизнесът и гражданите да бъдат подготвени за него. Общият регламент е законодателно отражение на най-голямата реформа на Европейския съюз по този въпрос.

Както е указано в 10-те практически стъпки за прилагане на Регламента, не следва да изчаквате за промени в националното законодателство, тъй като Регламентът става част от него, има пряко приложение и дава базисната правна рамка в сферата на защита на личните данни и личната неприкосновеност.

8. **До 25.05.2018 г. ли трябва общините да са готови с разработването, внедряването и евентуално сертифицирането на системата от документални и фактически процеси (технически и организационни мерки) за защита на данните.**

Считано от 25 май 2018 г. се отменя Директива 95/46/ЕО, която е транспонирана в действащия в момента Закон за защита на личните данни (ЗЗЛД). Това което следва да направите е да приведете досегашната дейност на общината, касаеща обработване и защита на лични данни, в съответствие с новите нормативни изисквания.

9. **Сертифицирането е доброволно, но колко ще струва за общините.**

Да, сертифицирането е доброволно, но също така то не води до намаляване на отговорността на администратора за спазване на Регламента и не засяга правомощията на надзорния орган /арг. чл 42, пара. 4/.

Създаването на механизми за сертифициране за защита на данните е в процес на разработка, като по-голяма яснота може да има след приемането на промени в законовите и подзаконовите нормативни актове.

10. **След като се разработи цялата система от документи за защита на личните данни на общината, трябва ли да бъде съгласувана с Комисията, преди да бъде внедрена.**

Извън изрично посочените случаи на съгласуване и консултиране по смисъла на Регламента, общината не следва да съгласува документацията си за защита на личните данни.

Такава е хипотезата на процедурата по предварителна консултация във връзка с оценка на въздействието по реда на чл. 36 от Регламента. Според разпоредбата администраторът се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаването му. Същото е възложено и като задача на длъжностното лице по защита на данните в чл. 39, пара. 1, бук. „д“ от Регламента.

Друга хипотеза е съгласуването на проект на кодекс за поведение /арг. чл. 40, пара. 5/.

В най-общ смисъл новата правна фигура на длъжностното лице по защита на данните следва да информира и съветва администратора и да наблюдава спазването на Регламента в неговата цялост.

11. **Какво представлява правото да бъдеш забравен и до каква степен е приложимо в общините.**

Регламентът въвежда редица изменения при обработването и защитата на личните данни. Съществена промяна по отношение на правата на гражданите е регламентирането на правото на изтриване (или „правото да бъдеш забравен“). Това право дава възможност, когато субектът на данни не желае данните му да бъдат обработвани и не съществуват законни основания за тяхното съхранение, те да бъдат заличавани.

По отношение на „правото да бъдеш забравен“, следва да се спомене Решението на Съда на Европейския съюз (ЕС) по казуса Google Spain (C-131-12), произнесено през май 2014 г., насочено към изясняване на няколко много важни въпроса, свързани с правото на субектите на лични данни да бъдат забравени, обективирано в

Директива 95/46/ЕО. Решението на съда предизвика широк отзвук и разнопосочни реакции както в ЕС, така и извън него, с оглед значението му за регулиране на дигиталното пространство. В него Съдът заключи, че извършваните дейности от търсачки (Google в конкретното решение) представляват обработване на лични данни, което може да засегне значително основните права на личен живот и на защита на личните данни, тъй като улеснява потребителите в изграждането на подробен профил на съответното лице.

Основният въпрос, който решението постави, е дали то е предпоставка за намирането на справедлив баланс между правото на лична неприкосновеност на лицата, свободата на изразяване, правото на достъп до информация и другите законни интереси на лицата в интернет пространството. Съдът счита, че с оглед на основната цел на Директива 95/46/ЕС, а именно да се осигури ефективна защита на основните права и свободи на физическите лица, и в частност на правото им на личен живот, тълкуването на разпоредбата, свързана с приложимостта на правото на ЕС не може да бъде ограничително. На това основание всяко лице, независимо дали е гражданин на държава-членка на ЕС, може да поиска от лицето, предоставящо услуги за търсене в интернет на територията на съответната държава-членка на ЕС, да бъдат заличени връзките към интернет страници, съдържащи информация, която нарушава неговите права, дори и в случаите, когато публикуването на информацията само по себе си е законно.

„Правото да бъдеш забравен“ е доразвито в Регламент (ЕС) 2016/679, като създава високо ниво на защита на личните данни. То е уредено в чл. 17 от Общия регламент. Съгласно пар. 1 на същия, субектът на данни може да поиска, а администраторът е длъжен да изтрие без ненужно забавяне конкретните лични данни. Горната възможност би могла да бъде осъществена единствено при наличието на следните основания:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- субектът на данните оттегля своето съгласие, върху което се основава обработването на данните;
- субектът на данни възразява срещу обработването и няма преимуществено законово основание за продължаване на обработването;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, което се прилага спрямо администратора;

- личните данни са били събрани във връзка с предлагането на услуги на информационното общество на дете.

Правото на изтриване е особено важно в последната хипотеза, а именно когато субектът на данни е дал съгласието си като дете и не е осъзнавал напълно рисковете, свързани с обработването. Впоследствие, ако лицето желае да премахне такива лични данни, то следва да може да упражни това право независимо от факта, че вече не е дете. Тази възможност е вследствие на основен принцип, залегнал в регламента, а именно завишената защита на личните данни по отношение на децата.

„Правото да бъдеш забравен“ като основно право в онлайн средата, следва да бъде разширено, като от администратора, който е направил личните данни обществено достъпни се изисква да уведоми администраторите, които обработват такива лични данни, да изтрият всякакви връзки към тези лични данни или техните копия или реплики. По този начин Регламент (ЕС) 2016/679 укрепва правото на изтриване, като пояснява, че организациите в онлайн средата, които правят личните данни публични, следва да информират други организации, които обработват личните данни, за да изтрият линковете или копията на въпросните лични данни. Въпреки че това може да е предизвикателство за администраторите, те трябва да се стремят да спазват тези изисквания. Те са длъжни да предприемат разумни мерки, вземайки предвид наличните технологии и средствата, с които разполагат, за да успеят да изпълнят задълженията си и да информират други администратори, които обработват лични данни, за искането на субекта на данните.

Все пак са налице са редица ситуации, в които администраторът има възможност да откаже да изтрие данните, а именно когато обработването на конкретните данни е с цел:

- да упражнява правото на свобода на изразяване и информация;
- да изпълнява правно задължение или да изпълнява задача от обществен интерес или упражняване на публична власт;
- за целите на общественото здраве;
- архивиране за цели в обществен интерес, научноизследователски исторически изследвания или статистически цели; или
- установяване, упражняване или защитата на правни претенции.

Предвид горното, „правото да бъдеш забравен“ не е абсолютно право. Всеки субект на данни може да се възползва от това си право единствено при наличие на конкретно основание.

12. **През какъв интервал от време следва да се преглежда оценката на риска за съответствие с Регламента.**

С цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на Регламента, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, материални или нематериални вреди.

В чл. 35, пара. 11 на Регламента е посочено, че при необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване. Извършването на оценка на риска, както и тази на въздействието, е непрекъснат процес и следва да се актуализира през целия „жизнен цикъл“ на защита на данните, с оглед спецификата и по решение на самия администратор.

13. **През какъв период следва да се извършват вътрешни одити на системата въз основа на Регламента и на вътрешните документи. От кого трябва да се извършват вътрешните одити.**

Преценката за вида и честотата на извършване на одити се прави от администратора на лични данни /арг. чл. 24 от Регламента/, като следва да се отбележи и функцията на длъжностното лице по защита на данните да наблюдава спазването на Регламента, политиките на администратора по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити.

14. **Какви ще бъдат санкциите за публичните органи.**

Общите условия за налагане на административни наказания „глоба“ или „имуществена санкция“ са разписани подробно в чл. 83 на Регламента.

Когато имуществената санкция се налага на предприятие, понятието „предприятие“ следва да се разбира като предприятие в съответствие с членове 101 и 102 от ДФЕС за тези цели. При налагане на административни наказания „глоба“ и „имуществена санкция“ на лица, които нямат качеството предприятие, надзорният орган следва да има предвид общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето, за да определи подходящия размер на глобата. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни наказания „глоба“ или „имуществена санкция“ /арг. съображение 150 от Регламента/.

За целите на антитръстовото законодателството на ЕС, всеки обект, който участва в икономическа дейност, т.е. дейност, при която има предлагане на стоки или услуги на даден пазар, независимо от неговото правно състояние и начина на финансиране, се нарича предприятие.

Във връзка с изложеното следва да се разгледа и понятието „публично предприятие“.

То е предприятие, при което публичните органи упражняват пряко или косвено контролиращо влияние по силата на своята собственост, финансово участие или ръководните правила. Контролиращо влияние на публичните органи е налице, когато те: а) притежават мнозинство от записания капитал на предприятието, б) контролират мнозинството от гласовете, прикрепени към акциите, емитирни от предприятието или в) са в положение, в което назначават повече от половината от членовете в административните, управленски или надзорните органи на дружеството.