****

**Практически въпроси на защитата на лични данни**

**в Община Смядово**

**От 25 май 2018 година във всички държави-членки ще се прилагат нови правила за защита на личните данни. Те са уредени в т. нар. Общ регламент за защита на личните данни (GDPR)**

****

**Целта на настоящата брошура е да разясни някои ключови въпроси, които да подпомогнат практическото прилагане на Общия регламент в Община Смядово.**

 Община Смядово, ЕИК 000 931 657, като публичен административен орган с административен адрес: гр. Смядово, пл. „Княз Борис І” №2, като администратор на лични данни, съгласно чл. 3 от Закона за защита на личните данни е вписана в „Регистъра на администраторите на лични данни и на водените от тях регистри администратор на лични данни, с идентификационен № 0051270.

Община Смядово обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели. Община Смядово поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на физическите лица за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.

**Данни за контакт с ОБЩИНА СМЯДОВО:**

Местоположение:

Държава: РЕПУБЛИКА БЪЛГАРИЯ

Адрес: гр. Смядово, пл.“Княз Борис І“ №2

Телефон: 05351/2033

Ел. поща: obshtina\_smiadovo@abv.bg

Интернет страница: http://www.smyadovo.bg/

Данни за контакт с Длъжностно лице по защита на данните

Ел. поща: dlzld@smyadovo.bg

Тел: 05351/2033

Съдържание:

**Съгласие за обработване на лични данни в Община Смядово ……………………………………………………….5**

**Право да бъдеш „забравен“ в Община Смядово ……………………………………………………………..…….6**

**Длъжностно лице за защита на личните данни в Община Смядово…………………………………………………….......7**

**Отчетност в Община Смядово………………………………9**

**Оценка на въздействието в Община Смядово**

**…………………………………………………………………..10**

**Защита на личните данни в Община Смядово на етап проектиране и по подразбиране**

**…………………………………………………………………..12**

**Административно-наказателна отговорност по Общия регламент………………………………………………………14**

**Съгласие за обработване на лични данни в Община Смядово**

 Съгласието е едно от алтернативните основания за законосъобразно обработване на лични данни. В Община Смядово под „ съгласие „ ще се разбира:

* Всяко свободно изразено – не е дадено под натиск и заплаха
* Конкретно - отделно съгласие за всяка цел
* Информирано – дадено е на основата на пълна, точна и лесно разбираема информация
* Недвусмислено – не се извлича или предполага въз основа на други изявления или действия



 Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между Община Смядово и субекта, за да е налице

съгласие. Съгласието на субекта за обработване на лични или специални категории данни се дава - въз основа на съответния документ за съгласие, предоставен от субекта на данни на Община Смядово за всяка конкретна цел на обработване. В повечето случаи, в ролята си на публично правен орган, основанието за обработка на лични и специални категории данни се получава на законово основание от Община Смядово, като се използват стандартни документи/бланки за предоставяне на административна услуга на гражданите на общината. Когато субектът подписва договор, съгласие не е необходимо, защото данните му се събират на друго законово основание.

 Когато Община Смядово обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 14, 16, 18 години.

**Правото да бъдеш забравен**

 Правото на изтриване (или “правото да бъдеш забравен”) дава възможност, когато субектът на данни не желае данните му да бъдат обработвани и не съществуват законни основания за тяхното съхранение, да поиска те да бъдат заличени при едно от 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 законово основание за продължаване на обработването;
* личните данни са били обработвани незаконосъобразно;
* личните данни трябва да бъдат изтрити с цел спазването на правно задължение;
* личните данни са били събрани във връзка с предлагането на услуги на информационното общество на дете.

 „Правото да бъдеш забравен“ не е абсолютно право. Съществуват ситуации, в които Община Смядово има възможност да откаже да изтрие данните, а именно когато обработването на конкретните данни е необходимо за някоя от следните цели:

* за упражняване правото на свобода на изразяване и информация;
* за изпълнение на правно задължение или на 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;
* за установяване, упражняване или защитата на правни претенции.

**Длъжностно лице по защита на данните**

 Длъжностното лице по защита на данните играе ключова роля за осигуряване на законосъобразното обработване на лични данни в структурата на администратора. То трябва да разполага с професионални качества и експертни познания в областта на защитата на личните данни (законодателство и практика). Основната задача на длъжностното лице е да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни. Важно е да се знае, че то не определя целите и средствата за обработване на данни и съответно администраторът не може да прехвърли своята отговорност за неспазване на изискванията .

 Общия регламент върху него. Поради тази причина длъжностното лице по правило не може да заема ръководни позиции, пряко свързани с обработването на лични данни в организацията на администратора, за да се избегне конфликт на интереси. В същото време длъжностното лице следва да разполага с висока степен на независимост, за да изпълнява ефективно своите консултативно-превантивни функции. Администраторът няма право да дава указания или нареждания във връзка с изпълнението на задачите на длъжностното лице по защита на данните, което следва да се отчита директно на висшия мениджмънт в организацията на администратора.



 Задължение да определят Длъжностно лице по защита на данните имат следните администратори на лични данни (физически и юридически лица):

* публичен орган или орган на местно самоуправление;
* администратори, които извършват мащабно обработване на специални (чувствителни) лични данни;
* в други, предвидени в закон случаи. Длъжностно лице по защита на данните може да изпълнява функциите си въз основа на един от следните алтернативни начини:
* назначаване на служител в дружеството или организацията;
* съвместяване с друга длъжност, стига да не се поражда конфликт на интереси.

**Отчетност**

 Отчетността е ново задължение на Община Смядово на лични данни и инструментът за доказване изпълнението на изискванията на Общия регламент за защита на личните данни. Отчетност на практика е способността във всеки един момент Община Смядово да удостовери и да докаже, че обработва личните данни законосъобразно, добросъвестно, прозрачно, за конкретни и пропорционални цели, с подходящо ниво на сигурност и защита. Основните средства за спазване на принципа на отчетност са:

• поддържането на регистри на дейностите по обработване в Община Смядово.

 • определяне на длъжностно лице по защита на личните данни.

 • извършване на оценка на въздействието при наличие на висок риск за правата и свободите на физическите лица.

 • своевременно уведомяване на Комисията за защита на личните данни и субекта на данните при нарушения на сигурността.



**Оценка на въздействието**

 Оценката на въздействието е важен инструмент при отчитането, защото помага на Община Смядово не само да спазва изискванията на Общия регламент за защита на личните данни, но и да демонстрират, че са предприети подходящи мерки, за да се гарантира спазването на регламента. Оценката на въздействието е процес, предназначен:

* да опише обработването на лични данни,
* да оцени необходимостта и пропорционалността на обработката й;
* да спомогне за избора на най-подходящите технически и организационни мерки за защита. Оценката на въздействието може да се отнася до единична операция за обработване на данни или до многобройни повтарящи се или сходни операции. Тя се изисква само когато обработването на лични данни има вероятност да доведе до висок риск за правата и свободите на физическите лица. Операции по обработване, които по правило пораждат висок риск, са например извършването на:
* автоматично вземане на решения, включително профилиране;
* мащабно обработване на данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация, както и данни за предишни осъждания на лицето;
* систематично мащабно наблюдение на публично достъпна зона

 

**Наблюдение и преглед**

**Оценка на необходимостта и пропорционалността**

**Документация**

**Предвидени мерки за доказване на спазването**

**Предвидени мерки за справяне с рисковете**

**Оценка на рисковете на правата и свободите**

Фиг. 1 Процеси за извършване ОВЗД

 Оценка на въздействието се извършва от Работната група на Община Смядово и задължително трябва да потърси съвет от служителя по защита на данните, когато такъв е определен, а взетите решения следва да бъдат документирани. Общият регламент за защита на личните данни определя минималното съдържание на оценката на въздействието:

* системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от Община Смядово законен интерес;
* оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;
* оценка на рисковете за правата и свободите на субектите на данни,
* мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент.

 Община Смядово задължително провежда предварителна консултация с КЗЛД, ако оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не се предприемат ефективни мерки за ограничаването му.

**Защитата на личните данни на етапа на проектирането и по подразбиране**



 Защитата на личните данни на етапа на проектирането и по подразбиране са нови задължения за администраторите на лични данни, въведени за първи път с Общия регламент за защита на данните. Независимо, че основната им цел е да се намалят и по възможност елиминират рисковете за личната неприкосновеност, прилагането им от администраторите на практика спомага за намаляване на евентуални последващи разходи за привеждане на информационните системи в съответствие с изискванията на регламента.

**Защитата на личните данни на етапа на проектирането** се изразява в задължението на администраторите да въведат подходящи технически и организационни мерки преди започването на обработката на лични данни (на етапа определяне

на целите и средствата за обработване), като осигурят тяхното прилагане през целия жизнен цикъл на данните. Изборът на конкретни технически и организационни мерки зависи изцяло от администратора, който следва да отчита достиженията на техническия прогрес, разходите за прилагане, естеството, обхвата, контекста и целите на обработването, както и породените

от обработването рискове с различна вероятност и тежест за правата и свободите на физическите лица. Такива подходящи мерки биха могли да бъдат псевдонимизация и/или криптиране на данните, залагане на функционалности за автоматизирано отчитане на сроковете за съхранение и автоматичното им изтриване след изтичането им и др.

 **Защита на личните данни по подразбиране** изисква администраторите да прилагат механизми, които по подразбиране гарантират изпълнението на следните изисквания:

* Само минималното количество лични данни и операции по обработване, които са абсолютно необходими за постигането на всяка специфична цел, биват обработвани.
* Данните са съхранявани за минималния срок, абсолютно необходим за постигане на целите на обработване (например, за периода необходим да се предостави съответния продукт или услуга) и след това заличени при спазване на съответните правила и процедури – според Номенклатурата на делата на Община Смядово.
* Всеки достъп, предаване или споделяне на данни е допустим, само при наличие на валидно правно основание за това (например, съгласието на субекта на данни или правни задължения на Община Смядово).

**Административно-наказателна отговорност по Общия регламент за защита на личните данни**



 Един от основните механизми за гарантиране спазването на високите стандарти на регламента от всички администратори, които са задължени да прилагат Регламент 2016/679, е възможността надзорните органи по защита на личните данни да налагат значителни по размер административни наказания. За осигуряване на ефективност, пропорционалност и възпиращ ефект регламентът въвежда следните критерии при определяне на вида административно наказание (парична санкция или друга

мярка) и неговия размер. Обстоятелствата, които се оценяват са следните:

* естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда;
* дали нарушението е извършено умишлено или по небрежност;
* действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни;
* степента на отговорност на администратора или обработващия лични данни, като се вземат предвид технически и организационни мерки, въведени от тях;
* евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни;
* степента на сътрудничество с КЗЛД с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него;
* категориите лични данни, засегнати от нарушението;
* начина, по който нарушението е станало известно на КЗЛД, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението;
* когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, във връзка със същия предмет на обработването, дали посочените мерки са спазени;
* всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението. При леки нарушения или ако глобата, която може да бъде наложена, представлява несъразмерна тежест за администратор - физическо лице, вместо глоба може да бъде приложена друга корективна мярка.

Източници:

1. <https://www.google.bg/search?q=%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82+%D0%BB%D0%B8%D1%87%D0%BD%D0%B8+%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8&hl=bg&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwiu8dr9hY3eAhUEDZAKHQzXC34Q_AUIDigB&biw=1366&bih=626#imgrc=63IMoAmosrldwM>:
2. <https://broxio.eu/2018/01/23/%D0%B8%D0%B7%D0%B8%D1%81%D0%BA%D0%B2%D0%B0%D0%BD%D0%B5-%D0%B7%D0%B0-%D0%B8%D0%B7%D1%80%D0%B8%D1%87%D0%BD%D0%BE-%D1%81%D1%8A%D0%B3%D0%BB%D0%B0%D1%81%D0%B8%D0%B5/>
3. <https://broxio.eu/2018/02/20/gdpr5-right-to-erasure/>
4. <https://www.rexecurity.com/gdpr-compliance-services/dpo-services-outsourcing-p142.htm>
5. <http://accountingnews.bg/%D0%BA%D0%B0%D0%BA-%D0%B4%D0%B0-%D1%81%D0%B5-%D1%81%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BC-%D1%81-%D0%BD%D0%BE%D0%B2%D0%B8%D1%8F-%D1%80%D0%B5%D0%B3%D0%BB%D0%B0%D0%BC%D0%B5%D0%BD%D1%82-%D0%B7%D0%B0-%D0%BB%D0%B8%D1%87%D0%BD%D0%B8%D1%82%D0%B5-%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8-gdpr-%D1%87%D0%B0%D1%81%D1%82-%D0%BF%D1%8A%D1%80%D0%B2%D0%B0-366.html>
6. <https://www.cpdp.bg/userfiles/file/WP29/wp248%20rev_01_bg.pdf>
7. <https://news.lex.bg/wp-content/uploads/2018/01/%D1%87%D1%83%D0%BA-%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D1%81%D1%8A%D0%B4%D0%B8%D0%B5.jpg>