



ОБЩИНА СИМИТЛИ, ОБЛАСТ БЛАГОЕВГРАД

П.к. 2730, гр. Симитли, ул. "Хр. Ботев" №27, тел. 0748/72138, 72157, факс: 0748/72231

ЗАПОВЕД

№ 271/09.07.2020г.

На основание чл.44, ал.2 от Закона за местното самоуправление и местната администрация, във връзка с прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016г. и чл.59, ал.2 от Закона за защита на личните данни

УТВЪРЖДАВАМ:

1. Политика за защита на личните данни на Община Симитли.
2. Вътрешни правила за защита на личните данни на Община Симитли.

Копие от заповедта да се връчи чрез електронна поща на всички заместник-кметове и директори на дирекции, кметове и кметски наместници за сведение и изпълнение.

Контрол по изпълнение на заповедта възлагам на Длъжностното лице по защита на личните данни.

АПОСТОЛ АПОСТОЛОВ
Кмет на Община Симитли



Ел.Г



ОБЩИНА СИМИТЛИ, ОБЛАСТ БЛАГОЕВГРАД

П.к2730, гр. Симитли, ул. "Хр. Ботев" 27, тел. 0748/72138, 72157, факс: 0748/72231

УТВЪРДИЛ,

АПСТОЛ АПОСТОЛОВ
КМЕТ НА ОБЩИНА СИМИТЛИ

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОБЩИНА СИМИТЛИ

Настоящата Политика за защита на личните данни не регламентира права и задължения, а има за цел да обясни защо и какви лични данни събираме, как ги обработваме, съхраняваме, в това число кога е необходимо да разкриваме лични данни на трети лица. С тази политика се предоставя информация за правата, които потребителите имат във връзка с обработването на лични данни от Община Симитли.

Обща информация

Считано от 25 май 2018 г. влиза в сила Регламент (ЕС) 2016/679 (General Data Protection Regulation – GDPR) 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 (Общ регламент относно защитата на данните). Регламентът урежда правата и задълженията по защита на личните данни на физическите лица от всички държави членки на ЕС.

Община Симитли е орган на местната власт, който във връзка със законовите си задължения да предоставя услуги на своите граждани и да следи за спазване на законодателството във важни сфери от обществения живот като гражданската регистрация, гражданското състояние, устройството на територията, общинската собственост, местните данъци и такси, обществения ред и т.н., събира, обработва, използва и съхранява лични данни.

Община Симитли в качеството си на администратор на лични данни по смисъла на чл. 4, ал. 7 от Регламент (ЕС) 2016/679 осъществява дейността по събиране, обработване и съхранение на лични данни в съответствие с Регламент (ЕС) 2016/679 и Закона за защита на личните данни.

Данни за контакт с Община Симитли:

гр. Симитли- п.к. 2730, ул. "Христо Ботев" № 27

Електронна поща: simitly@mail.bg

Интернет страница: www.simitli.bg

Телефон: 0748/72138

Данни за контакт с длъжностното лице по защита на данните:

По всички въпроси, свързани с обработването на Вашите лични данни и с упражняването на права, можете да се обърнете към определеното от Кмета на Община Симитли длъжностно лице по защита на данните на телефон: 0748/72138; електронна поща: simitly@mail.bg

Правно основание за обработването

Във връзка с качеството си на публичноправен субект в голямата част от своята дейност, Община Симитли обработва лични данни на основание спазване на законово задължение за администратора.

Административните услуги, които предлагаме изискват обработване и съхранение на лични данни. Тези данни са необходими, за да бъде обработена и изпълнена съответната услуга според нормативната уредба на Република България и Европейския съюз. Община Симитли събира личните данни за конкретни, легитимни цели и личните данни не се обработват по-нататък по начин, несъвместим с тези цели.

Лични данни се събират във връзка със:

- спазване на законови задължения;
- изпълнение на договори;
- изпълнение на задачи от обществен интерес;
- упражняване на служебни правомощия;
- защита на законни интереси

Как обработваме личните данни

Обработването обхваща широк спектър от операции, извършвани с лични данни, включително с ръчни или автоматични средства. Това включва събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване на личните данни.

Как и какви лични данни събираме за потребителите

В повечето случаи получаваме информация директно от субектите на данни, когато те попълват искания, заявления и други документи, необходими за упражняването на официалните правомощия и за спазване на законови задължения на общинската администрация. Лични данни получаваме и от трети страни, например публични органи.

Личните данни, които се събират от Община Симитли са:

- три имена;
- единен граждански номер (личен номер на чужденец);
- адрес;
- място на раждане;
- пол;
- данни от документ за самоличност;
- данни за пълномощник и за неговото пълномощно (ако лицето се представлява от пълномощник);
- данни за здравословно състояние;
- семеино положение;

- родствени връзки;
- деца;
- образование;
- трудов опит;
- свидетелство за съдимост;
- професионална квалификация;
- данни за обратна връзка със субектите на данни – пощенски адрес, адрес на електронна поща, телефонен номер и др.

Във връзка с разпоредбата на чл.9 от Регламент (ЕС) 2016/679 Община Симитли не събира и не обработва лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, както и обработването на генетични и биометрични данни, данни за сексуалния живот или сексуалната ориентация на физически лица. Личните данни от тази категория ще събираме, обработваме и съхраняваме единствено, когато това ни е вменено по закон или сме получили вашето изрично съгласие за това и при строго съблюдаване на член 9, § 2 от Регламент (ЕС) 2016/679.

Срокове за съхранение на личните данни

Многообразието от услуги, които Община Симитли предоставя, изисква и различен срок за съхранение на лични данни на хартиен/електронен носител, чиито критерии са определени от нормативната уредба в страната. Съхраняваме личните Ви данни до изпълнение на целта, за която са събрани или съобразно сроковете, посочени в закони, наредби и други нормативни актове. След постигане на целите, за които са събрани данните, след изтичане на срока за съхранение, по искане на субекта на данните(ако е приложимо) или ако обработката е била незаконосъобразна, данните се унищожават.

Получатели или категории получатели на лични данни

Категориите получатели на които Община Симитли предоставя лични данни извън организацията:

- На публични органи (Национална агенция по приходите, Национален осигурителен институт, Министерство на вътрешните работи, органи на съдебната власт, контролни органи, органи на местното самоуправление и т.н.);
- На обработващ лични данни (физическо или юридическо лице, което обработва личните данни от името на Община Симитли, по нареждане или възлагане).
- Банки (с оглед изплащане на дължимите възнаграждения на служителите на администратора)
- Доставчици на пощенски и куриерски услуги при адресиране на кореспонденция до физически лица.
- И други категории получатели, които имат законово право да събират, обработват и получават лични данни.
- Община Симитли не разкрива лични данни за целите на директния маркетинг.

Община Симитли не разкрива вашите лични данни на трети лица без предварително да получи Вашето съгласие, с изключение на случаите когато по закон е длъжна да го прави. Получатели на вашите данни най-често са органи на държавна власт, които получават, обработват и съхраняват лични данни въз основа на конкретни и ясни законови задължения. Община Симитли може да предаде вашите лични данни поддоставчици на услуги, които са сключили договор с нея.

Принципи при събирането, обработването и съхраняването на лични данни

При обработката, събирането и съхраняването на лични данни, Община Симитли се ръководи от следните принципи:

- Законосъобразност, добросъвестност и прозрачност;
- Съотносими с целите на обработка и свеждане до минимум на събираните данни;
- Ограничение на целите на обработване;
- Точност и актуалност на данните;
- Ограничаване срока на съхранение на документи с лични данни;
- Цялостност и поверителност на обработването и гарантиране на подходящо ниво на сигурност на личните данни.

Когато за обработването на лични данни не е налице друго основание, личните данни на физическите лица, се обработват след като бъде получено тяхното свободно и информирано съгласие за това. В случаите, когато се обработват данни на лице под 14 години, това обработване е законосъобразно само и доколкото това съгласие е дадено или разрешено от упражняващия родителски права родител или от настойника на субекта на данните. За изпълнение и доказване на изпълнението на задължението за свободно и информирано съгласие, физическите лица(субектите на данните) подписват **Декларация за съгласие за обработване на лични данни (Приложение №1 и №3 към “Вътрешни правила за защита на личните данни,,)**.Субекта на данни по всяко време има възможност да оттегли своето съгласие за обработване на данни, като подаде **Декларация за оттегляне на съгласие за обработване на лични данни (Приложение №2 към “Вътрешни правила за защита на личните данни“)**. Личните данни се събират за конкретни, точно определени от закона или от Община Симитли(по изключение)цели. Допустима е единствено допълнителна обработка за целите на архивирането или статистически цели, в които случаи не е налице несъвместимост на поставените цели. Община Симитли не изисква да бъдат предоставяни повече от необходимите данни. Обемът на изискуемите данни в повечето случаи е нормативно определен.

Когато е налице правно основание за обработване на лични данни, различно от съгласието, напр. нормативно задължение или договор, Община Симитли не следва да дублира това основание със съгласие на лицето.

Права на субектите на лични данни

Субект на лични данни е физическо лице, което е идентифицирано или което може да бъде идентифицирано въз основа на определена информация.

Според Регламент (ЕС)2016/679 за защита на личните данни субектът на данни има право на:

- Информираност (във връзка с обработването на личните му данни от администратора) чл.13 от Регламент(ЕС)2016/679;
- Достъп до собствените си лични данни (чл.15 от Регламент(ЕС)2016/679);
- Коригиране (в случай че данните са неточни) чл.16 от Регламент(ЕС)2016/679;
- Изтриване на личните данни (право “да бъдеш забравен“) чл.17 от Регламент (ЕС)2016/679;
- Ограничаване на обработването (чл.18 от Регламент(ЕС)2016/679);
- Право на преносимост на данните (чл.20 от Регламент(ЕС)2016/679);
- Възражение срещу обработването на негови лични данни (чл.21 от Регламент(ЕС)2016/679);
- Автоматизирано вземане на индивидуални решения, включително профилиране (субекта на данните има право да не бъде обект на решение, основаващо се единствено

на автоматизирано обработване, включващо профилиране, което поражда правни последици за субекта на данните или по подробен начин го засяга в значителна степен(чл.22 от Регламент(ЕС)2016/679);

Изискванията към процедурата, по която субекта на лични данни може да реализира правата си по чл.15 – 22 от Регламент(ЕС) 2016/679 са в съответствие със Закона за защита на личните данни. Всеки субект на лични данни може да упражни своите права чрез подаването на писмено заявление/искане (Приложение №4 към “Вътрешни правила за защита на личните данни“) в сградата на Община Симитли с адрес: гр. Симитли, ул. “Христо Ботев“№27, лично или чрез пълномощник с нотариално заверено пълномощно. Съгласно чл.37в, ал.2 от Закона за защита на личните данни, когато вносителя на заявлението/искането е упълномощено лице, към заявлението се прилага и пълномощното. Заявление/искане може да бъде подадено и по електронен път при условията на Закона за електронния документ и електронните удостоверителни услуги, Закона за електронното управление и Закона за електронната идентификация.

При необходимост, когато администраторът има основателни опасения относно самоличността на физическото лице, подало искане за упражняване на свои права, той може да поиска предоставянето на допълнителна информация от него с цел установяване по безспорен начин на идентичността на субекта на данни.

Личните данни, обработвани във връзка с разглеждането на отделните искания ще се използват само за целите на упражняване на посочените права.

*** 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 преимуществено законово основание за продължаване на обработването;
- Личните данни са били обработвани незаконосъобразно;
- Личните данни трябва да бъдат изтрети 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 Симитли 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.

Технически и организационни мерки за защита на личните данни

Община Симитли организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване. Общинската администрация прилага мерки за защита на личните данни, които осигуряват: физическа защита(контрол на достъп до сгради, помещения, съоръжения и др.), персонална защита(поемане на задължение за опазване на поверителността на личните данни, извършване на обучения, тренировки на персонала),документална защита(вътрешни правила за документооборота, правила за дейността, правила за размножаване и разпространение на лични данни на хартиен носител и др.),защита на автоматизираните информационни системи и/или мрежи и др.

Средства за правна защита

Субекта на данни има право на защита по административен или съдебен ред, в случай, че правата му са били нарушени.

Надзорен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент(ЕС) 2016/679 и на Закона за защита на личните данни е Комисията за защита на личните данни с адрес за кореспонденция: гр. София 1592, бул. „Проф. Цветан Лазаров“ №2, телефон: 02/91 53 519, интернет страница: www.cpdp.bg

Значение на основните понятия по смисъла на чл. 4 от Регламент (ЕС) 2016/679 и Закона за защита на личните данни.

1. „Администратор“ е физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;
2. „Лични данни“ са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“);
3. „Обработващ лични данни“ е физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора и е лице, различно от администратора;
4. „Субект на данните“ е идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано;
5. „Физическо лице, което може да бъде идентифицирано“ е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

6. **„Чувствителни лични данни”** лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическото лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице;
7. **„Съгласие на физическото лице”(субекта на данните)** представлява ясен утвърдителен акт, с който се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни. Например чрез писмена декларация, включително по електронен път или устна декларация;
8. **„Предоставяне на лични данни”** са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея;
9. **„Обработване на лични данни”** е всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, поддръждане или комбиниране, ограничаване, изтриване или унищожаване;
10. **„Получател”** е физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на държавата членка, не се считат за получатели. Обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;
11. **„Оторизирано лице”** е лице, което по силата на естеството на преките си служебни задължения и/или изрично оторизиране, има право за достъп до определена категория за лични данни;
12. **„Регистър за лични данни”** е всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;
13. **„Псевдонимизация”** е обработване на лични данни по такъв начин, че личните данни не могат повече да бъдат свързани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на техническа и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;
14. **„Трето лице”(страна)** означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;
15. **„Анонимизиране”** е процес, в резултат на който, се създава информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице по такъв начин, че субектът на данните да не може или вече не може да бъде идентифициран;
16. **„Нарушение на сигурността на личните данни”** е нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;
17. **„Носител на лични данни”** е физически обект, на който могат да се запишат данни или могат да се възстановят от същия

§ Настоящата Политика за защита на личните данни се приема на основание чл.24, параграф 2 от Регламент (ЕС) 2016/679 (General Data Protection Regulation – GDPR) 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 (Общ регламент относно защитата на данните).

§ Всички служители на общинска администрация, чиито служебни задължения включват обработване на лични данни, са длъжни да се запознаят с настоящата Политика и да я спазват.

§ Община Симитли запазва правото си да изменя и допълва внедрената Система за защита на личните данни и средствата за защита на личните данни, в съответствие с настъпилите промени в приложимото законодателство, развитието на технологиите за защита, като това може да стане по инициатива на Община Симитли или на компетентен орган(Комисията за защита на личните данни).

§ Настоящата Политика за защита на личните данни влиза в сила от деня на утвърждаването ѝ от Кмета на Община Симитли.



ОБЩИНА СИМИТЛИ, ОБЛАСТ БЛАГОЕВГРАД

пк 2730 – гр. Симитли, ул. "Хр. Ботев" № 27, тел. 0748/7-21-38, 7-21-57, факс: 0748/7-22-31

УТВЪРДИЛ,

АПОСТОЛ АПОСТОЛОВ
КМЕТ НА ОБЩИНА СИМИТЛИ

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ОБЩИНА СИМИТЛИ

Глава първа Общи положения

Раздел I Предмет и обхват

Чл.1(1) Настоящите Вътрешни правила за защита на личните данни уреждат организацията на обработване и защита на лични данни на физическите лица, получени при осъществяването, както на основната, така и на поддържащата дейност на Община Симитли, по отношение на които последната е администратор или обработващ лични данни.

(2) Правилата са изготвени в съответствие с изискванията на Регламент(ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и отмяна на Директива 95/46/ЕО(Общ регламент относно защитата на данните).

(3) Вътрешните правила са предназначени за всички служители, които в рамките на служебните си задължения обработват лични данни, на които Община Симитли е администратор или обработващ лични данни.

Чл.2 (1) Настоящите Правила уреждат:

1. процедурите, механизмите и принципите за обработка на личните данни;
2. процедурите за администриране на искания за достъп до данни, коригиране на обработвани данни, възражения и оттегляне на съгласия, както и администриране на искания за упражняване на други права, които субектите на лични данни имат право по закон;
3. процедурата за действие при нарушаване на сигурността на личните данни;

(2) Неразделна част от настоящите Вътрешни правила са всички процедури, механизми, правила, мерки и съобщения за поверителност във връзка със защитата на личните данни на физическите лица, получени при осъществяването, както на основната, така и на поддържащата дейност на Община Симитли.

Раздел II Информация за администратора

Чл.3(1) Община Симитли с ЕИК 000024987 и адрес: гр. Симитли 2730, ул. "Христо Ботев" №27 има качеството на администратор на лични данни по отношение на лични данни, обработването на които е необходимо за изпълнение на функциите ѝ.

(2) Кметът на Община Симитли в качеството си на публичен орган определя длъжностно лице по защита на личните данни.

Раздел III Длъжностно лице по защита на личните данни

Чл.4(1) Основната цел на определеното от Кмета на Община Симитли длъжностно лице по защита на личните данни е да подпомага администратора на лични данни и неговите служители в прилагането на изискванията за защита на личните данни, като ги информира и съветва за техните задължения, произтичащи от Регламент(ЕС)2016/679 и други правни актове на ЕС и вътрешното право на Република България.

(2) Длъжностното лице по защита на личните данни докладва директно на Кмета на Община Симитли и Секретаря на Общината.

(3) Длъжностното лице по защита на личните данни изпълнява следните задачи:

- а) информира и съветва служителите на Община Симитли за задълженията, свързани с обработването на лични данни, съгласно законодателството в областта на личните данни и настоящите Вътрешни правила;
- б) изпълнява задълженията си по докладване и управление на нарушения на сигурността на данните;
- в) наблюдава спазването на законодателството в областта на защита на данните и настоящите Вътрешни правила по отношение на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване и съответните одити;
- г) осъществява сътрудничеството на Община Симитли с Комисията за защита на личните данни;
- д) консултира физическите лица във връзка с обработването на лични данни от Община Симитли, приема и обработва постъпили искания за упражняване на права;

(4) Данните за контакт с длъжностното лице по защита на личните данни се обявяват на лесно достъпно място на електронната страница на Община Симитли, както и в съобщенията за поверителност.

Глава втора Субекти на данни и категории лични данни

Раздел I Субекти на данни

Чл.5(1) Община Симитли събира и обработва лични данни, необходими за осъществяване на своите права и задължения като публичен орган, работодател, доставчик на услуги и контрагент при съблюдаване изискванията на приложимото законодателство.

(2) Личните данни, които се събират от Община Симитли са:

- три имена;
- единен граждански номер (личен номер на чужденец);
- адрес;
- място на раждане;
- пол;
- данни от документ за самоличност;
- данни за пълномощник;
- данни за здравословно състояние;
- семейно положение;
- родствени връзки;
- деца;
- образование;
- трудов опит;
- свидетелство за съдимост;
- професионална квалификация;

-данни за обратна връзка със субектите на данни – пощенски адрес, адрес на електронна поща, телефонен номер и др.

(3) Община Симитли обработва специални категории лични данни, само доколкото това е необходимо за изпълнение на специфичните ѝ права и задължения по закон.

Раздел II

Достъп до лични данни

Чл.6(1) Достъпът до лични данни в Община Симитли се осъществява при прилагане на принципа “Необходимост да се знае”.

(2) Право на достъп до носителите на лични данни имат само лицата които:

а) изпълняват служебните си задължения съгласно трудовия договор или договора за държавна служба и длъжностната характеристика за съответната длъжност или съгласно др. вид договор;

б) са оторизирани чрез изричен акт;

в) изпълняват сключени с Община Симитли договори;

(3) Лицата, които имат достъп до лични данни носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на носителите, съдържащи лични данни.

Глава трета

Принципи за защита на личните данни

Раздел I

Чл.7(1) В качеството си на администратор на лични данни Община Симитли и всички служители, които в рамките на служебните си задължения обработват лични данни, спазват следните принципи:

1. Принцип на законосъобразност, добросъвестност и прозрачност.

2. Принцип на ограничение на целите.

3. Принцип на свеждане на данните до минимум.

4. Принцип на точност.

5. Принцип на ограничение на съхранението.

6. Принцип на цялостност и поверителност.

7. Принцип на отчетност.

(2) Принципите изброени в ал.1 се прилагат кумулативно.

(3) Спазването на принципите се осъществява през целия “жизнен цикъл“ на данните – от създаването/получаването им до тяхното изтриване или унищожаване на техните носители.

Раздел II

Законосъобразност

Чл. 8 (1) В изпълнение на принципа за законосъобразност, общинската администрация, обработва лични данни само при наличие на основание за обработката.

(2) Лични данни се обработват при наличие на поне едно от следните основания:

а) обработването е необходимо, за сключване на договор (предприемане на стъпки за сключване на договор по молба на субекта на данните) или е необходимо във връзка с изпълнението на вече сключен договор – напр. на това основание ще се изискват и обработват лични данни при сключване на договор със служителите;

б) обработването е необходимо за изпълнение на определено законово задължение – по правило дейността на общинската администрация е правно регламентирана, поради което това е най-често използваното основание, въз основа на което се обработват лични данни;

в) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, напр. при предаване на данни необходими за опазване на живота или здравето на лицето.

Чл.9 (1) Когато за обработването на лични данни не е налице друго основание, личните данни на физическите лица, се обработват след като бъде получено тяхното информирано съгласие за това.

(2) За да бъде легитимно, съгласието трябва да отговаря едновременно на следните критерий:

1. Да бъде свободно изразено.

2. Да е конкретно

3. Да е информирано.

4. Да е недвусмислено.

5. Да е изрично изявление или ясно потвърждаващо действие.

(3) В случаите, когато се обработват данни на деца под 14 години, това обработване е законнообразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.

(4) За изпълнение и доказване на изпълнението на задължението за информирано съгласие по смисъла на ал. 1, субектите на данни подписват Декларация за съгласие по образец /Приложение № 1и №3 към настоящите Вътрешни правила/.

(5) Общинската администрация осигурява възможност на субекта на данни по всяко време да има възможността да оттегли своето съгласие за обработване на данни, като подаде Декларация за оттегляне на съгласие /Приложение № 2 към настоящите Вътрешни правила./.

Чл.10 (1) За изпълнение на конкретно определени цели общинската администрация обработва различни категории лични данни.

(2) Обработване на специални категории лични данни се извършва само в случаите, когато:

а) субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели;

б) обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, дотолкова, доколкото това е разрешено от правото на Съюза или националното законодателство, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните;

в) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

г) обработването е свързано с лични данни, които явно са направени обществено достойствие от субекта на данните;

д) обработването е необходимо с цел установяване, упражняване или защита на правни претенции;

е) обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или националното законодателство, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;

ж) обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на социалните услуги на нормативно основание;

з) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;

и) обработването е необходимо от съображения от обществен интерес в областта на общественото здраве.

Раздел III

Добросъвестност и прозрачност.

Чл. 11(1) В изпълнение на изискванията за добросъвестност и прозрачност на обработката на лични данни, Община Симитли обработва данните „честно и открито” спрямо субектите на данни.

(2) Община Симитли спазва точният баланс между вида и обема/количеството на личните данни, които се обработват, причините, поради които администраторът обработва данните и информацията, която е дал на субекта на данни за това.

(3) Информиранието на субектите на данни се извършва чрез Съобщение за поверителност за конкретна обработка, което съдържа следната информация: данни за контакт с Община Симитли, данни за контакт с длъжностното лице по защита на данните, обхват, цел и адресати на съобщението за поверителност, категории лични данни и категории субекти на които се

обработват данни, правно основание и цели на обработването, източници за събиране на лични данни, информация за срока на съхранението на данните, разкриване и трансфер на данни,

автоматизирано вземане на решения и профилиране, мерки за сигурност на данните, информация за упражняване правата на субектите на данни.

(4) Общинската администрация създава и периодично актуализира най – малко следните Съобщения за поверителност:

а) Съобщение за поверителност на личните данни на общинските съветници в Общински съвет Симитли;

б) Съобщение за поверителност на личните данни на служителите и други лица, чиито данни се обработват във връзка с управление на човешките ресурси и финансово – счетоводната отчетност;

в) Съобщение за поверителност на кандидатите за работа;

г) Съобщение за поверителност на личните данни при приемане на жалби, сигнали и предложения на граждани

д) Съобщение за поверителност на личните данни при изпълнение на законови задължения(Политика) ;

(5) В случаите на проектиране на нова обработка се преценява необходимостта от изготвяне на Съобщение за поверителност за тази обработка.

(6) Длъжностното лице по защита на данните прави периодичен преглед на дейностите по обработка на данни и дава указания за изготвяне на Съобщения за поверителност.

Раздел IV

Законово определяне на целите и допълнителна обработка.

Чл. 12 (1) Личните данни се събират за конкретни, изчерпателно посочени и разграничени една от друга точно определени от закона /по правило/ или от общинската администрация /по изключение/ цели.

(2) Личните данни не се обработват допълнително по начин, несъвместим с тези цели.

(3) Допустима е единствено допълнителна обработка за целите на архивирането в обществен интерес или за статистически цели, в които случаи не е налице несъвместимост на поставените цели.

Раздел V

Свеждане на данните до минимум.

Чл.13 Общинската администрация не изисква предоставянето на повече данни от необходимите. Обемът на изискуемите данни в повечето случаи е нормативно определен.

Раздел VI

Точност.

Чл. 14 (1) Общинската администрация предоставя възможност за актуализиране на неточни и непълни данни по реда за упражняване на правото на коригиране, описан в Процедурата за упражняване на права на субектите на данни.

(2) Коригиране се извършва и по друг ред, когато това е предвидено в нормативната уредба на дейността на Общинската администрация.

Раздел VII

Ограничение на съхранението.

Чл. 15 (1) Личните данни се съхраняват на хартиен и/или електронен носител, само за времето, необходимо за постигане на преследваните цели.

(2) При наличие на нормативно определени срокове Община Симитли съхранява данните за определения в нормативен акт период.

(3) Правилата за съхранение, включително срокът за съхранение, както и правилата за унищожаване, когато такива не са определени в нормативната уредба, се определят с Вътрешните правила за организация на административната дейност.

(4) След постигане на целите, за които са събрани, след изтичане на срока за съхранение, по искане на субекта на данните /ако е приложимо/ или ако обработката е била незаконосъобразна,

данните се унищожават, независимо от вида на носителя им, по начин, който не позволява възстановяването им.

Раздел VIII

Сигурност на обработваното (цялостност и поверителност)

Чл. 16 (1) Общинската администрация организира и предприема мерки за защита на личните данни от случайно или незаконно унищожаване, от неправомерен достъп, от изменение или разпространение, както и от други незаконни форми на обработване.

(2) Предприеманите мерки са съобразени със съвременните технологични постижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени.

Чл. 17 (1) Общинската администрация прилага мерки за защита на личните данни, които осигуряват: физическа защита, персонална защита, документална защита, защита на автоматизирани информационни системи и/или мрежи, криптографска защита, защита на личните данни при отношения с трети страни и доставчици.

(2) Служителите на Община Симитли, кметове на кметства и кметски наместници, стажанти, лица по гражданско правоотношение подписват Споразумение за конфиденциалност за обработваните от тях лични данни .

(3) Общинските съветници в ОбС Симитли подписват Споразумение за конфиденциалност за обработваните от тях лични данни .

Раздел IX

Нарушения на сигурността на личните данни.

Чл. 18 (1) Принципът за цялостност и поверителност при обработването на лични данни се реализира и чрез осигуряване на адекватни действия на служителите в случай на нарушения на сигурността.

(2) Описание на необходимите действия, които трябва да бъдат предприети от ръководството и служителите от администрацията на Община Симитли за постигане на ефективно управление на нарушенията на сигурността на личните данни се съдържа в Процедура за действие при нарушение на сигурността на личните данни.

(3) Общинската администрация уведомява Комисията за защита на личните данни и засегнатите субекти на данните /когато е необходимо съгласно нормативните изисквания/ за нарушението на сигурността на личните данни.

Раздел X

Документиране

Чл. 19(1) В изпълнение на принципа за отчетност, общинската администрация документира изпълнението на всички свои задължения.

(2) Цялата документация е достъпна в системата за вътрешен документооборот.

Раздел XI

Унищожаване на данните

Чл. 20(1) Унищожаване на лични данни се извършва от Общината и/или от изрично упълномощено лице, без да бъдат накърнявани правата на лицата, за които се отнасят данните, обект на унищожаването и при спазване на разпоредбите на относимите нормативни актове.

(2) Информацията в регистрите се унищожават след постигане на целите на обработка и при отпаднала необходимост от съхранение.

(3) Унищожаването на документи от архивните фондове на Общината става само след разрешение на органите за управление на Държавния архивен фонд и при спазване на Закона за защита на личните данни.

Глава четвърта

Права на физическите лица

Чл. 21 (1) Физическите лица, чиито данни се обработват от общинската администрация в качеството ѝ на администратор, имат следните права при обработване на отнасящи се за тях лични данни: право на информация, право на достъп до данните, право на коригиране, право на

изтриване/правото „да бъдеш забравен“, право на ограничаване на обработването, право на възразение, право да не бъде обект на автоматизирано вземане на индивидуални решения, включително профилиране, право на преносимост на данните, право на жалба до надзорния орган.

(2) Всяко физическо лице, личните данни на което ще се обработват от администратора, следва да бъде уведомено чрез Съобщението за поверителност, съгласно чл.11, ал.4 от настоящите Вътрешни правила.

(3) Уведомяване по смисъл на ал.2 не се извършва, когато:

- а) обработването е за статистически цели и предоставянето на информацията е невъзможно или изисква прекомерни усилия;
- б) физическото лице, за което се отнасят данните, вече разполага с информацията;
- в) обработката е предвидена в закон;
- г) е налице изрична нормативна забрана.

(4) Условието и реда за упражняване правата на субекта на данни, с изключение на правото на жалба до надзорния орган се съдържат в Процедура за упражняване на права от субектите на данните .

Глава пета

Сигурност на личните данни при обработка от трети лица

Чл.22(1)Община Симитли може при необходимост да предостави лични данни на трети лица, действащи в качеството на администратор или обработващ, въз основа на изричен договор/споразумение или нормативен акт.

(2)В случаите на предоставяне на лични данни на служители, потребители или доставчици на услуги, община Симитли:

- а)изисква достатъчно гаранции от обработващия/администратора за спазване на законовите изисквания и добрите практики за обработка и защита на личните данни;
- б)сключва писмено споразумение или друг правен акт с идентично действие, който урежда задълженията на администратора/обработващия и отговаря на изискванията на чл.28 от Регламент(ЕС) 2016/679.

(3)Копие от договора /споразумението по ал.1 се предоставя задължително на Длъжностното лице по защита на данните.

Глава шеста

Регистър на дейностите по обработка

Чл. 23 (1) Общинската администрация поддържа постоянно Регистър на дейностите по обработка на данни.

(2) Регистърът на дейностите по обработка се поддържа в писмена форма, включително в електронен формат.

(3) Достъп до регистъра имат всички служители, ангажирани с дейности по обработка на личните данни. При поискване длъжностното лице по защита на личните данни предоставя достъп до регистъра на Комисията за защита на личните данни.

Глава седма

Оценка на въздействието върху личните данни

Чл.24(1) В процеса на обработване на лични данни общинската администрация отчита рисковете с различна вероятност и тежест за правата и свободите на физическите лица, които могат да настъпят при обработване на личните им данни.

(2)Действията на общинската администрация при извършване на преценката на риска, които са от решаващо значение за определяне на подходящи организационни и технически мерки за защита, следват следната последователност:

анализ на риска → определяне нивото на сигурност → прилагане на подходящи мерки за сигурност

(3) Общинската администрация извършва оценка на въздействието, когато обработката създава висок риск за правата и свободите на физическите лица.

(4)Анализа на риска, който се създава при обработването на лични данни общинската администрация основава на определени обективни критерии, а именно: естеството на обработване на лични данни, обхват на обработването, контекст на обработването и целта на обработването.

(5) На базата на извършената по ал. 2 оценка на риска се изготвя план за действие, който съдържа необходимите механизми за контрол, отговорните лица и сроковете за изпълнение .

Чл.25(1) Оценка на въздействието задължително се извършва при обработване на лични данни получени чрез системи за видеонаблюдение.

Чл.26 В случаите когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, а последиците от този риск не могат да бъдат намалени, общинската администрация се консултира с Комисията за защита на личните данни преди обработването.

Глава осма

Предоставяне на данни в трети държави и международни организации

Чл.27(1) Общинската администрация предоставя лични данни в трети страни или на международни организации при спазване на изискванията на Регламента.

(2) Правилата и условията за предаване на лични данни на трети държави или международни организации от Община Симитли, в качеството на администратор на лични данни се уреждат в Процедура за предаване на лични данни на трети държави или международни организации.

Глава девета

Защита по проектиране и по подразбиране

Чл.28 (1) При планиране и предоставяне на нови услуги общинската администрация осигурява защита по проектиране и подразбиране съгласно изискванията на Регламента за защита на данните, освен ако дейностите по обработка са предвидени в нормативен акт.

(2) Прилагането на изискванията за „Защита на личните данни по проектиране“ и „Защита на личните данни по подразбиране“ изисква мерките за защита на данните да бъдат взети под внимание на всички етапи от жизнения цикъл на личните данни и на всички етапи на конкретен проект (проектиране, одобряване и внедряване), на всички процеси (проекти, приложения или начини на работа), които определят обработката на лични данни при осъществяване на дейността на общинската администрация.

(3) Изискването за осигуряване на „Защита на личните данни по проектиране“ включва редица фактори, които трябва да бъдат взети под внимание от всички структурни звена на общинската администрация, отговорни за обработката на лични данни.

(4) За осигуряване на „Защита на личните данни по проектиране“, общинската администрация прилага принципите за защита на личните данни, както следва:

а) при планиране на всяка дейност по обработка на данни ясно се дефинира и документира целта на дейността. При разглеждането на целите на обработката на данни се отчита как и по отношение на кои лица е било извършено информирането за използването на личните им данни. В случаите когато новата дейност представлява нова /допълнителна/ обработка на лични данни, се изисква уведомяване на физическите лица чрез Съобщение за поверителност. Ако не е налице друго основание за новата обработка, следва да бъде поискано тяхното съгласие.

б) при планиране на всяка дейност по обработка следва да:

-се установи точният обем на данните, необходими за определената цел;

- се планира обработка само на лични данни, необходими за осъществяване на законната и определена цел;

- не се включва обработка на лични данни само защото са лесно достъпни /например от съществуваща база данни/ или защото за тях може да се счита, че е „добре да ги има“ или да имат бъдеща, неопределена полезност.

- се събират и обработват личните данни само за минималния брой лица, необходими за ефективността на планирания процес.

в) при планиране на всяка дейност по обработка, следва да се:

- планира необходимостта от анонимизиране на данните или сигурното им изтриване веднага щом вече не се изискват /при липса на конкретно законово изискване да се съхраняват данните за по-дълго време/;