Приложение № 6 към Заповед № 359/ 23.05.2018 г.

ВЪТРЕШНИ ПРАВИЛА
за получаване, обработване, съхраняване и защита на лични данни в община Тервел

I. Раздел. Предмет

Чл. 1.(1) С настоящите вътрешни правила се урежда минималното ниво на техническите и организационни мерки в Община Тервел за защита на личните данни при тяхното получаване, обработване и съхраняване в поддържаните регистри.

(2) Вътрешните правила се утвърждават на основание Закона за защита на личните данни, в съответствие с Регламент за защита на личните данни 2016/679 /ОРЗД/, обнародван в Официален вестник на Европейския съюз от 04.05.2016 год., в сила от 23.05.2018 год.

(3) Тези правила се утвърждават, изменят, допълват и отменят от кмета на Община Тервел.

Чл. 2. Вътрешните правила регламентират:

1.механизмите за съхраняване, обработване и защита на личните данни, съдържащи се в поддържаните от общинската администрация регистри с цел осигуряване на неприкосновеност на личния живот на гражданите;

2. видовете регистри, които се водят в Община Тервел и тяхното описание;

3. необходимите технически и организационни мерки за защита на личните данни, съдържащи се в регистрите от неправомерен достъп и други незаконни форми на обработване;

4. статута и задълженията на администратора длъжностното лице по защита на личните данни, обработващите лични данни или работещите под тяхно ръководство, както и отношенията на тези лица с администратора;

5. въвеждането на системи за контрол на достъпа, работно време и трудов ата дисциплина във връзка с обработването и защитата на личните данни.

II. Раздел. Лични данни

Чл. 3.(1) Лични данни са всяка информация, свързана с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано, пряко или непряко чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор, или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социалната идентичност на това физическо лице.

(2) Личните данни се събират за конкретни, изрично указани и легитимни цели, обработват се законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните и не могат да се обработват допълнително по начин, несъвместим с целите.

(3) Личните данни се съхраняват във форма, която да позволява идентифициране на субекта на данните за период, не по – дълъг от необходимото за целите, за които тези данни се обработват. Личните данни могат да се съхраняват и за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, при условие, че бъдат приложени подходящите мерки, за да се гарантират правата и свободите на субекта на данните.

III. Раздел. Обработване на лични данни

Чл. 4.(1) Обработване на личните данни е всяка операция или съвкупност от операции, извършвани с личните 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, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(2) Обработване на личните данни се състои и в осигуряване на достъпа до определена информация. То се извършва само от лица, чиито служебни задължения или конкретно възложена задача предвижда това.

(3) Обработването на лични данни е допустимо само в случаите , когато е налице някое от следните основания:

1. физическото лице, за което се отнасят данните, е дало изрично своето съгласие да бъдат обработени – съгласието се дава само лично и е недвусмислено;

2. изпълнение на нормативно установено правомощие или функция на администратора на лични данни или на трето лице, на което се разкриват данните;

3. обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия предхождащи сключването на договор и предприети по негово искане;

4. обработването е необходимо, за да се защитят животът и здравето на физическото лице, за което се отнасят данните;

5. обработването е необходимо за изпълнението на задача на администратора, която се осъществява в обществен интерес;

6. обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, с изключение на случаите, при които над тези интереси преимущество имат интересите на физическото лице, субект на данните.

(4) Основанията по т.1-6 от предходната алинея се прилагат при условията на алтернативност. Съгласие по ал.3, т.1 не се изисква при наличие на поне едно от останалите основания.

(5) Основанието по чл. 4, ал.3, т.6 не може да се прилага за случаи, при които Община Тервел изпълнява своите задачи като публичен орган.

Чл. 5.(1) Представляващият администратора със заповед възлага обработването на личните данни на служители в администрацията. Обработването се възлага на повече от един обработващ данните, съобразно спецификата на изпълняваните функции и с цел разграничаване на конкретните им задължения.

(2) Обработването на лични данни се възлага според регистрите, посочени в **Приложение № 1** към настоящите правила.

(3) Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.

Чл. 6. Субектите на лични данни се информират за необходимостта от набиране на лични данни и целите, за които ще бъдат използвани при условията на чл.12, § 1, във връзка с чл.13 и чл. 14 от ОРЗД.

Чл.7. Личните данни в регистрите се набират от администратора на лични данни съответно от обработващият лични данни чрез устно интервю и/или на хартиен носител.

Чл.8.(1) Свободен публичен достъп до информация, съдържаща ЕГН/ЛНЧ не се допуска, освен ако закон предвижда това.

(2) В случаите, в които публичните услуги се заявяват от субектите на данните пред Община Тервел по електронен път, освен ЕГН/ЛНЧ администраторът определя и второ средство за идентификация на потребителя при предоставяне на отдалечен достъп до съответната услуга, което се вписва в съответните входящи дневници.

(3) Документ за самоличност, свидетелство за управление на моторно превозно средство и документ за пребиваване могат да бъдат копирани само, ако закон предвижда това.

Чл. 9.(1) След одобрение на документите, съдържащи лични данни от ресорния ръководител, същите заедно с приложенията към тях се обработват в регистрите от обработващ лични данни.

(2) Набраните данни на технически носител остават в отделни файлове на компютъра, като достъп до тях има само обработващ лични данни.

(3) Хартиеният носител се подрежда в кадрови досиета или специални папки и се представя за проверка законосъобразността на изготвения документ и валидирането му чрез подписи на съответните длъжностни лица.

(4) За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.

Чл.10. Относно режима на обработване на лични данни в Община Тервел при създаване на фотографско или аудио-визуално произведение чрез заснемане на лице в хода на обществената му дейност; след приключване на процедура по набиране и подбор на персонал; на починало лице; за целите на Националния архивен фонд или за научни и статистически изследвания или за статистически и хуманитарни цели се прилагат съответните разпоредби на Закона за защита на личните данни.

IV. Раздел. Видове регистри

Чл. 11.(1) В поддържаните в Община Тервел регистри на личните данни се събират и съхраняват данни за:

1. физическите лица в Република България;
2. физически лица – граждани на друга държава;
3. служителите на трудово и служебно правоотношение в администрацията.

(2) Категориите лични данни в регистрите, които се отнасят до физическите лица могат да бъдат относно:

- физическа идентичност - име, постоянен и настоящ адрес, ЕГН/ЛНЧ, номер, дата и място на издаване на документ за самоличност, месторождение, телефони за връзка, електронна поща, подпис и др.;
- семейната идентичност - семейно положение (наличие на брак, развод, брой на членове на семейството, в т.ч. деца до 18 години), родствени връзки и др.;
- образование - вид на образованието, място, номер и дата на издаване на диплома; допълнителна квалификация;
- трудова дейност; професионална биография;
- медицински данни - физиологично, психическо и психологично състояние на лицата;
- икономическа идентичност - размер на трудовото възнаграждение, вещни права, участие в търговски дружества, регистрация като едноличен търговец, кредити, задължения за данъци и такси, здравни и социални осигуровки, ценни книжа и др.

(3) Видовете регистри с лични данни, които се водят в Община Тервел са описани в Приложение по чл. 6, ал. 2 от Процедура за водене и поддържане на регистър на дейностите по обработване на лични данни в Община Тервел, представляващо неразделна част към Приложение № 3 към Заповед № 359/ 23.05.2018 г. на Кмета на Община Тервел. Приложението съдържа и нивата на защита на поддържаните от Община Тервел регистри/програмни продукти.

(4) Приложението по ал. 3 се допълва, изменя или отменя със заповед на кмета на общината.

V. Раздел. Начин на водене на регистрите

Чл. 12. Личните данни от лицата се подават до администратора на личните данни, както и до лицата, определени за обработване на лични данни по реда на чл.5, ал.1.

Чл. 13.(1) Информацията, съдържаща лични данни на хартиен носител се съхранява в папки, които се подреждат в специални картотечни шкафове. Предоставянето, промяната или прекратяването на неоторизиран достъп до регистри се контролира от секретаря на Община Тервел.

(2) Картотечните шкафове могат да бъдат поставени в помещения, предназначени за самостоятелна работа на обработващия лични данни или в общи помещения за работа с изпълняващи други дейности.

(3) Личните данни за всяко лице се набират в изпълнение на нормативно задължение – разпоредбите на закони, кодекси, подзаконови нормативни актове и други чрез:

- устно интервю с лицето;
- хартиен носител - писмени документи – съобщения, преписи от актове, молби, заявления, лични документи по текущи въпроси в процеса на работа, подадени от лицето или предоставени по служебен път;
- външни източници (от финансови, административни, съдебни и други органи).

(4) При публикация или обявяване на населението на проекти или издадени заповеди и други актове на общината, кметът на общината или други служители, съдържащите се в тях лични данни се заличават чрез псевдонимизация, инициали или по друг подходящ начин.

Чл. 14.(1) Достъп до лични данни има само обработващият ги и действащо под пряко негово ръководство оторизирано длъжностно лице.

(2) Обработващият данните се задължава да не предоставя достъп до предоставените му за обработка данни на трети лица, освен в предвидените от закона случаи.

(3) Обработващият данните изготвя и представя на администратора списък на оторизираните да оперират с данните служители, представляващ неразделна част към настоящите вътрешни правила, оформен като Приложение № 1 към същите.

Чл. 15.(1) Формата на организация и съхраняване на личните данни на технически носител се осъществява чрез тяхното въвеждане на твърд диск на сървъри от компютърната мрежа или на изолиран компютър. Компютърът е свързан в локалната мрежа, със защитен достъп до личните данни, с който може да работи само обработващ лични данни при мерки с високо или средно ниво.

(2) При работа с данните се използват съответните софтуерни продукти за обработка. Те могат да бъдат адаптирани към специфичните нужди на администратора.

(3) Достъп до файловете за обработка на лични данни имат само работещите с тях. Носители с лични данни могат да се разпространяват само ако е използван друг механизъм, гарантиращ, че данните не могат да се четат или променят при пренасянето им.

(4) Защита на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява чрез :

1. поддържане на антивирусни програми;
2. периодично архивиране на данните на отделни електронни носители;
3. съхраняване на информацията на хартиен носител.

(5) Когато данните се намират на изолирани компютри архивирането им се извършва от оператора на съответния компютър (обработващия лични данни).

VI. Раздел Оценка на въздействието върху защитата на данните

Чл. 16.(1) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството обхвата и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

(2) При извършването на оценка на въздействието върху защитата на данните администраторът иска становището на длъжностното лице по защита на личните данни при Община Тервел.

(3) Оценката по ал.1 се извършва пореда на чл.35 от ОРЗД.

VII. Раздел. Технически и организационни мерки за гарантиране нивото на сигурност

Чл. 17.(1) Администраторът на личните данни предприема необходимите технически, и организационни мерки, за да защити данните от случайно или незаконно използване, загуба или друга форма на незаконно обработка.

2) Администраторът взема специални мерки за защита, когато обработването включва предаване на данните по електронен път.

(3) Мерките по ал. 1 и 2 са съобразени със съвременните технологични постижения и осигуряват ниво на защита, което съответства на рисковете, свързани с обработването, и на естеството на данните, които трябва да бъдат защитени.

Чл. 18.(1) Техническите мерки за гарантиране нивото на сигурност са:

1. компютърните сървъри за база данни да са на съвременно техническо ниво; Сървърния хардуер да използва RAID технологии за дискова подсистема, hot-swap твърди дискове и оперативна памет с механизъм за откриване и корекции на грешки.

2. .компютърните работни конфигурации да използват Desktop операционни системи съобразно изискванията на приложния софтуер за работа с лични данни, да са компетентно балансирани и функционално оптимизирани;

3. за всички компютърни конфигурации, сървъри и комуникационни средства, от които зависи правилното поддържане на базите с лични данни, следва да бъдат осигурени непрекъсваеми токозахранващи устройства (UPS);

4. минималния набор от системни програмни средства на всяка работна компютърна конфигурация включва :

- операционна система съобразно изискванията на ползвания приложен софтуер с инсталирани пакети за сигурност;
- антивирусен софтуер с включено автоматично обновяване и постоянно сканиране;
- активирана защитна стена.

5. гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

6. редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки;

7. сътрудничество с Комисията за защита на личните данни /КЗЛД/ при изпълнение на задълженията, произтичащи по регламента.

(2) Достъпът до компютърната мрежа и до софтуера за работа с лични данни се осъществява от длъжностни лица със специални кодове /пароли/;

(3) Администраторът предприема мерки за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент.

Чл. 19. Организационните мерки за гарантиране на нивото на сигурност са:

1.със заповед на представляващия администратора се определят обработващите лични данни за различните видове регистри, които се водят при администратора;

2.организира се охрана на работните помещения в рамките на охраната на цялата сграда чрез оперативни дежурни;

3. работните компютърни конфигурации, както и цялата IT инфраструктура, включително и достъпът до интернет, се използват единствено за служебни цели;

4. пренасянето на лични данни през интернет се осъществява само чрез служебна електронна поща; забранено е използването на лични електронни пощи за пренос на лични данни;

5. забранено е използването на преносими лични носители на данни /диск, флаш-памет/ в звената от администрацията, в които се обработват лични данни;

6. при ремонт на компютърна техника, на която се съхраняват лични данни, предоставянето й на сервизната организация се извършва без устройствата, на които се съхраняват лични данни;

7. прилагане на псевдонимизация на предоставените за обработване лични данни;

8. при внедряване на нов програмен продукт за обработване на лични данни, следва със заповед на представляващия администратора да се състави комисия по тестване и проверка възможностите на продукта, с оглед спазване изискванията на Закона за защита на личните данни и осигуряване на максималната им защита от неправомерен достъп, загубване, повреждане или унищожаване.

VIII. Раздел. Администратор на лични данни и обработващ на лични данни

Чл. 20.(1) Администратор на лични данни е Община Тервел, представлявана от кмета на Община Тервел.

(2) Администраторът на лични данни като отчита естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност е тежест с правата и свободите на физическите лица, прилага подходящи физически и организационни мерки, предвидени в тези правила, ЗЗЛД и ОРЗД, за да гарантира и да е в състояние да докаже, че обработването се извършва законосъобразно.

(3) Предвидените в тези правила мерки се преразглеждат и актуализират при необходимост.

(4) Администраторът – Община Тервел прилага и подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването и без намеса от страна на субекта на данните личните данни не са достъпни за неограничен брой физически лица /"защита на данните по подразбиране"/.

(5) Звената на администратора обменят лични данни при спазване на нормативните изисквания и във връзка с изпълнение на функциите си.

Чл. 21.(1) Администраторът може да обработва данните сам или чрез възлагане на обработващ данните.

(2) Администраторът може да възложи обработването на лични данни от негово име само на обработващи лични данни, които предоставят достатъчно гаранции, че ще прилагат подходящи технически и организационни мерки по такъв начин, че обработването да отговаря на изискванията на ОРЗД и ЗЗЛД и да се гарантира защитата на правата на субекта на данните.

(3) Когато е необходимо по организационни причини, обработването може да се възложи на повече от един обработващ, включително с цел разграничаване на конкретните им задължения и според обособеността на водените регистри.

(4) Обработващите лични данни се определят със заповедта по чл.5, ал.1.

Чл. 22.(1) Обработващият лични данни се задължава:

1. да спазва тези правила, както и да изпълнява задълженията си по ОРЗД и ЗЗЛД;
2. да обработва личните данни само по документирано нареждане на администратора;
3. да подпомага администратора;
4. да поддържа възложения му регистър от база данни;
5. да осигурява сигурността на личните данни чрез извършване на подходящи мерки;
6. да ограничи достъпа до помещенията, в които се съхраняват данните само за оторизираните служители /монтиране на специални шкафове, заключване на помещенията/ и др.;
7. да осигури достъп до електронните бази данни само по отношение на оторизираните служители /дефиниране на права на достъп до нивата, пароли за достъп до програмната среда, пароли за отваряне на файловете/;
8. да осигури подходяща защита на електронните данни чрез активиране на антивирусна защита, поддържане на резервно копие и др.

9. да гарантира, че намиращите се под негово ръководство служители са поели ангажимент за поверителност;
10. да информира незабавно администратора при нарушения;
11. да изпълнява други задължения, предвидени в ОРЗД, ЗЗЛД и тези правила.
(2) Обработващият не може да превъзлага свои функции на трети лица.

Чл. 23. Обработващият лични данни подписва декларация, че е запознат и ще спазва изискванията на ОРЗД, Закона за защита на личните данни и настоящите правила, която е неразделна част от настоящата като **приложение №2.**

Чл.24.(1) Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите. Тези лица са действащи под ръководството на администратора или обработващия лични данни по смисъла на чл.29 от ОРЗД.

(2) Действащите под ръководството на администратора и обработващия лица обработват лични данни само по документирано указание на администратора.

(3) Лицата по чл. 29 от ОРЗД в Община Тервел също подписват декларация – приложение №2.

Раздел X. Длъжностно лице по защита на личните данни

Чл.25.(1) Длъжностното лице по защита на личните данни се определя с административен акт на представляващия администратора. То има статут по чл.37-39 от ОРЗД.

(2) Длъжностното лице по защита на лични данни участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни в Община Тервел.

(3) Длъжностното лице по защита на личните данни:

1. информира и съветва, администратора, обработващите лични данни и лицата, които извършват обработване на лични данни под ръководството на администратора и обработващия лични данни по въпроси на приложението на ОРЗД и Закона за защита на личните данни;

2. да наблюдава спазването на правилата и политиките за защита на личните данни;

3. при поискване предоставя съвети във връзка с изготвени оценки на въздействието;

4. да изисква от администратора изпращане на уведомление до КЗЛД при нарушения на сигурността на ЛД;

5. да съгласува отговори по постъпили искания за реализация на права.

6. сътрудничи и действа като точка за контакт на КЗЛД;

7. осъществява вътрешни одити и проверки за спазване на ОРЗД и ЗЗЛД;

8. изпълнява и други задачи възложени му с регламента, ЗЗЛД и тези вътрешни правила.

(4) Администраторът осигурява технически и организационно дейността на длъжностното лице по защита на личните данни по защита на личните данни, включително необходимите ресурси, достъп до личните данни и операциите по обработването, както и поддържането на неговите експертни знания.

XI. Раздел. Контрол на достъпа, работно време и трудова дисциплина

Чл. 26.(1) Достъп до лични данни, предоставени за обработка от субект на данни, имат само администратора, обработващия, длъжностни лица намиращи се под ръководство на администратора или обработващите и длъжностното лице по защита на лични данни.

(2) Лични данни на хартиен и електронен носител могат да се съхраняват и обработват само в работни помещения на администрацията на Община Тервел.

(3) Достъпът до работните помещения е ограничен и контролиран от дежурните на входа на сградата. Когато в работното помещение няма служител, то се заключва.