Одобрявам ,

Директор на РЗИ - Шумен
Д-р Пепа Калоянова
Дата: 26.06.2019 г.

ВЪТРЕШНИ ПРАВИЛА/ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В РЕГИОНАЛНА ЗДРАВНА ИНСПЕКЦИЯ – ШУМЕН

Разработил и отговорен за актуалното състояние на документа: Роза Кирилова – главен юрисконсулт в дирекция „АПФСО”

Шумен , м. 06.2019 г.

ГЛАВА ПЪРВА
ОБЩИ ПОЛОЖЕНИЯ.

Информация за администратора

Чл. 1. (1) Регионална здравна инспекция – Шумен (РЗИ – Шумен) с ЕИК по Булстат: 176031145 и адрес: гр. Шумен, п.к. 9700, област Шумен, пл.„Освобождение” №1 има качеството „администратор на лични данни“ по отношение на личните данни, обработването, на които е необходимо за изпълнение на функциите ѝ съгласно Регистъра на дейностите по обработка.

(2) В качеството си на публичен орган РЗИ - Шумен определя длъжностно лице по защита на личните данни.

(3) Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

а) информира и съветва РЗИ - Шумен за задълженията, свързани с обработването на лични данни, съгласно законодателството в областта на защита на данните и настоящите Вътрешни правила.

б) наблюдава спазването на законодателството в областта на защита на данните и настоящите Вътрешни правила 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.

в) при поискване предоставя съвети по отношение на оценката на въздействието върху защитата на данните и наблюдава извършването на оценката.

г) осъществява сътрудничеството на РЗИ - Шумен с Комисията за защита на личните данни.

д) консултира физическите лица във връзка с обработването на лични данни от инспекцията, приема и обработва постъпили искания за упражняване на права.

(4) Данните за контакт с длъжностното лице по защита на данните се обявяват на лесно достъпно място на електронната страница на РЗИ - Шумен, както и в Съобщенията за поверителност.

Предмет

Чл. 2. (1) Настоящите Вътрешни правила за защита на личните данни (наричани за краткост „Вътрешни правила“ или „Политики“) уреждат организацията на обработване и защитата на лични данни на физическите лица, получени при осъществяването, както на основната, така и на поддържащата дейност на РЗИ - Шумен, по отношение на които последната е администратор.

(2) Вътрешните правила са предназначени за всички служители, които в рамките на служебните си задължения обработват лични данни, на които РЗИ - Шумен е администратор.

Достъп до лични данни

Чл. 3. (**1**) Достъпът до лични данни в РЗИ - Шумен се осъществява при прилагане на принципа „Необходимост да знае”.

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

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

б) които са оторизирани чрез изричен акт;

в) които изпълняват сключени с РЗИ - Шумен договори.

(3) Достъп се предоставя след запознаване с нормативната уредба в областта на защитата на личните данни, правилата и процедурите за защита на личните данни и опасностите за личните данни, обработвани от администратора.

(**4**) Оторизираните с право на достъп лица подписват Споразумение за

конфиденциалност на лични данни, до които са получили достъп при и по повод изпълнение на задълженията им, съгласно чл.13, ал.4 и ал.5 от настоящите Вътрешни правила.

(5) 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. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни може да бъде основание за прилагане на трудово дисциплинарни мерки или да ангажира гражданска отговорност, а в определени случаи – и наказателна отговорност.

ГЛАВА ВТОРА
ПРИНЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ.

Раздел I
ЗАКОНОСЪОБРАЗНОСТ, ДОБРОСЪВЕСТНОСТ И ПРОЗРАЧНОСТ

Законосъобразност (Основания за обработката на лични данни)

Чл. 4. (1) В изпълнение на принципа за законосъобразност, РЗИ - Шумен, 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 при сключване на договор със служителите;

б) обработването е необходимо за изпълнение на определено правно задължение – по правило дейността на РЗИ - Шумен 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. 5 (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) В случаите, когато се обработват данни на деца под 14 години, това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.

(3) 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 № 1*** към настоящите Вътрешни правила)**.**

(4) РЗИ - Шумен 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. 6 (1) За изпълнение на конкретно определени цели РЗИ - Шумен обработва различни категории лични данни.

(2) Обработване на чувствителни 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 достояние 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 трудовата медицина, за оценка на трудоспособността на служителя или за целите на управлението на социалните услуги, на нормативно основание;

з) обработването е необходимо за целите на архивирането в обществен интерес, или за статистически цели.

Добросъвестност и прозрачност

Чл. 7. (1) В изпълнение на изискванията за добросъвестност и прозрачност на обработката, съгласно които за лицата следва да е ясно по какъв начин отнасящи се до тях лични данни се събират, използват, или обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данните, РЗИ - Шумен информира субектите на данните за тази обработка.

(2) Информирането на субектите на данни се извършва чрез Съобщение за поверителност за конкретна обработка, което съдържа следната информация: данни за контакт с РЗИ - Шумен, данни за контакт с длъжностното лице за 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 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.

(3) РЗИ - Шумен създава и периодично актуализира най-малко следните Съобщения за поверителност:

а) 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 ***(Приложение №3.1);***

б) Съобщение за поверителност на кандидатите за работа ***(Приложение №3.2)***;

в) Съобщение за поверителност на личните данни при приемане на жалби, сигнали и предложения на гражданите***(Приложение №3.3);***

г) Съобщение за поверителност на личните данни, създадени чрез системата за видеонаблюдение на РЗИ - Шумен ***(Приложение №3.4);***

д) Съобщение за поверителност на личните данни при изпълнение на законови задължения (***Приложение №3.5***);

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

(5) 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 II
ОПРЕДЕЛЯНЕ НА ЦЕЛИТЕ, СВЕЖДАНЕ НА ДАННИТЕ ДО МИНИМУМ, ТОЧНОСТ, ОГРАНИЧЕНИЕ НА СЪХРАНЕНИЕТО

Законово определяне на целите и допълнителна обработка

Чл. 8. (1) Личните данни се събират за конкретни, точно определени от закона (по правило) или от РЗИ - Шумен (по изключение) цели.

(2) 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.

Свеждане на данните до минимум

Чл. 9. РЗИ - Шумен не изисква предоставянето на повече данни от необходимите. Обемът на изискуемите данни в повечето случаи е нормативно определен.

Точност

Чл. 10. (1) РЗИ - Шумен предоставя възможност за актуализиране на неточни и непълни данни по реда за упражняване на правото на коригиране, описан в Процедурата за упражняване на права от субекта на данните по чл.16, ал.2 от настоящите Вътрешни правила.

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

Ограничение на съхранението

Чл. 11. (1) Личните данни се съхраняват на хартиен и/или електронен носител, само за времето, необходимо за изпълнение на дейностите за обработката им и/или нормалното й функциониране, освен ако според законите на Р. България не се изисква друг период за съхранението им.

(2) 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/Политика за съхранение на лични данни ***(Приложение №4).***

(3) 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. Редът за унищожаване е определен във Вътрешните правила/Политика за съхранение на лични данни, съгласно ал. 2.

Раздел III
ЦЯЛОСТНОСТ И ПОВЕРИТЕЛНОСТ

Сигурност на обработването

Чл. 12. (1) РЗИ - Шумен 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. 13. (1) РЗИ - Шумен 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) Мерките за защита на личните данни се описват подробно в документ с наименование „*Организационните и технически мерки за защита на личните данни“* (***Приложение №5*** към настоящите правила).

(3) Служителите на РЗИ - Шумен, лица по гражданско правоотношение подписват Споразумение за конфиденциалност за обработваните от тях лични данни (***Приложение №5.1*** към настоящите правила).

(4) Договорни партньори на РЗИ - Шумен подписват Споразумение за конфиденциалност за обработваните от тях лични данни (***Приложение №5.2*** към настоящите правила).

Нарушения на сигурността на личните данни

Чл. 14. (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 РЗИ - Шумен 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 (**Приложение №** **6** към настоящите правила).*

(3) РЗИ - Шумен 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 IV
ОТЧЕТНОСТ

Документиране

Чл. 15.(1) В изпълнение на принципа за отчетност, РЗИ - Шумен документира изпълнението на всички свои задължения.

(2) Цялата документация е достъпна в системата за вътрешен документооборот, както и при Длъжностното лице по защита на данните.

ГЛАВА ТРЕТА
ПРАВА НА ФИЗИЧЕСКИТЕ ЛИЦА

Чл. 16. (1) Физическите лица, чиито данни се обработват от РЗИ - Шумен 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/право „да бъдеш забравен“, Право на ограничаване на обработването, Право на възражение, 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, чийто лични данни ще се обработват от администратора, следва да бъде уведомено чрез Съобщението за поверителност, съгласно чл. 7, ал. 2 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) Условията 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 (**Приложение № 7** към настоящите правила).*

ГЛАВА ЧЕТВЪРТА
СИГУРНОСТ НА ЛИЧНИТЕ ДАННИ ПРИ ОБРАБОТКА ОТ ТРЕТИ ЛИЦА

Чл. 17. (1) РЗИ - Шумен изисква осигуряване на адекватни технически и организационни мерки от обработващите от негово име лични данни, които са включени в съответния акт с всеки обработващ.

(2) Условията, при които обработващият извършва от името на РЗИ - Шумен операциите по обработка на данни се дефинират и конкретизират в *Споразумение за обработване на лични данни (**Приложение №8** към настоящите Вътрешни правила).*

(3) Преди сключване на споразумението, обработващият следва да покаже необходимото ниво на защита на лични данни, съгласно нивото на защита, определено от РЗИ - Шумен като попълни карта за съответствие на обработката на лични данни, неразделна част от Споразумението по ал. 2.

ГЛАВА ПЕТА
РЕГИСТЪР НА ДЕЙНОСТИТЕ ПО ОБРАБОТКА

Чл. 18. (1) РЗИ - Шумен 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.

(4) Действията и отговорните лица, ангажирани със създаването и поддържането на Регистър на дейностите по обработка на лични данни от РЗИ - Шумен се определят с *Процедура за създаване и поддържане на регистър на дейностите по обработка на личните данни (**Приложение №9** към настоящите Вътрешни правила)*

ГЛАВА ШЕСТА
ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЛИЧНИТЕ ДАННИ

Чл. 19. (1) РЗИ - Шумен извършва оценка на въздействието, когато обработката създава висок риск за правата и свободите на физическите лица.

(2) Оценката на риска на операциите по обработване на лични данни в РЗИ - Шумен се извършва по утвърдена Методика за оценка на риска, съгласно изискванията на стандарта ISO 31000 (***Приложение №10*** към настоящите Вътрешни правила).

(3) 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 (***Приложение № 11*** към настоящите Вътрешни правила).

Чл. 20. Оценката на въздействието се извършва съгласно *Процедурата за извършване на оценка на въздействието върху личните данни* (***Приложение № 12*** към настоящите Вътрешни правила) и *Методология за извършване на оценка на*

въздействието (***Приложение № 1*** към Процедурата за извършване на оценка на въздействието върху личните данни).

Чл. 21 (1) Оценка на въздействието задължително се извършва при обработване на лични данни, създадени от изградени от РЗИ - Шумен системи за видеонаблюдение.

(2) Редът, начина за обработване и защита на личните данни, създадени чрез системите за видеонаблюдение на РЗИ - Шумен се уреждат с *Правила за обработване, съхранение и защита на лични данни при видеонаблюдение в сградата на* РЗИ - Шумен (***Приложение № 13*** към настоящите Вътрешни правила).

(3) В случаите когато оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако не бъдат предприети мерки за ограничаване на риска, РЗИ - Шумен се консултира с Комисията за защита на личните данни преди обработването.

ГЛАВА СЕДМА
ПРЕДОСТАВЯНЕ НА ДАННИ В ТРЕТИ ДЪРЖАВИ И МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Чл. 22. (1) РЗИ - Шумен предоставя лични данни в трети страни или на международни организации. при спазване на изискванията на Регламента и съгласно Процедурата за предоставяне на лични данни в трети държави.

(2) Правилата и условията за предаване на лични данни на трети държави или международни организации от РЗИ - Шумен, в качеството на администратор на лични данни се уреждат в *Процедура за предаване на лични данни на трети държави или международни организации* (***Приложение № 14*** към настоящите Вътрешни правила).

ГЛАВА ОСМА
ЗАЩИТА ПО ПРОЕКТИРАНЕ И ПО ПОДРАЗБИРАНЕ

Чл. 23. (1) При планиране и предоставяне на нови услуги РЗИ - Шумен осигурява защита по проектиране и подразбиране съгласно изискванията на Общия регламент 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 РЗИ - Шумен.

(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 РЗИ - Шумен, отговорни за обработката на лични данни.

(4) За осигуряване на „Защита на личните данни по проектиране“, РЗИ - Шумен 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 е 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 съгласието.

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

1. се установи точният обем на данните, необходими за определената цел;
2. се планира обработка само на лични данни, необходими за осъществяване на законната и определена цел;

3. 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 е да ги има“ или да имат бъдеща, неопределена полезност.

4. 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:

1. 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);

2. осигури възможност различните типове данни да могат да бъдат изтрити по различни периоди от време, в зависимост от съответната цел, без да се засяга качеството на останалите данни;

3. вземе предвид мястото, където ще се съхраняват данните.

г) При планирането на всяка дейност по обработка е необходимо:

1. да се ограничи достъпът до лични данни само до лицата (служители или доставчици на услуги), за които е необходимо да имат достъп до личните данни за определените им задачи, и единствено в изпълнение на определената цел на процеса.

2. достъпът до личните данни трябва да се следи, така че нарушенията на личните данни да могат по-лесно да бъдат открити и проследени, ако е технически осъществимо. Всяко такова проследяване трябва да се изпълнява по начин, който отчита правото на защита на личните данни на служителите или на третите лица, доставчици на услуги (както и на техните служители).

д) При планирането на всяка дейност по обработка е необходимо:

1. да се осигури анонимизиране или псевдонимизиране на личните данни, ако не е необходимо директно да се идентифицират определени лица;

2. да се гарантира, че мерките за сигурност се прилагат във връзка с всички дейности по обработка на данни, които са предназначени да осигурят ниво на сигурност на данните, което е подходящо за конкретните рискове от дейността по обработка на данни. За изпълнението на това изискване е необходимо да се измерят конкретните рискове. Когато се очаква рискът за физическите лица от обработващата дейност да е висок, се извършва оценка на въздействието върху защитата на данните.

е) При планирането на всяка дейност по обработка трябва да се гарантира, че РЗИ - Шумен е в състояние да създаде възможност за упражняване на всички права на субектите на данни.

(5) За съответствието на всяка планирана обработка с принципите на Общия регламент за защита на данните и изискванията по ал. 4 се извършва анализ и оценка на съответствието, съгласно *Методика за оценка на съответствието (**Приложение № 15*** към настоящите Вътрешни правила*).*

(6) Отговорност за осигуряване на „Защита на личните данни по проектиране“ и „Защита по подразбиране“ носи ръководителят на организационното звено, което планира извършването на процеса или предоставянето на услугата.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§.1 В настоящия документ понятията се използват със следното значение:

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. **„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.

3. „**Лични данни“** са всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“);

4. **„Нарушение на сигурността на лични 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.

5. „**Носител на лични данни**” е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.

6. „**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, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

7. „**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;

8. „**Оторизирано лице**“ е лице, което по силата на естеството на преките си служебни задължения и/или изричното оторизиране, има право за достъп до определена категория лични данни;

9. „**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 държава 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.

10. „**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.

11. **„Псевдонимизация“** е обработване на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически 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.

12. „**Регистър на 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. „**Регламент**“ – 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 и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните);

14. „Субект на данните“ е идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано;

15. „**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;

16. „**Трето лице (страна)**“ е 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.

17. **„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 физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

18. **„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 физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§. 1 Настоящите Вътрешни правила се приемат на основание член 24, параграф 2 от 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 и за отмяна на Директива.

§. 2 Всички служители на РЗИ - Шумен, чиито служебни задължения включват обработване на лични данни, са длъжни да се запознаят с настоящите Вътрешни правила и да ги спазват. Запознаването се удостоверява с подпис.

§. 3. Настоящите Вътрешни правила се публикуват на официалната страница на РЗИ - Шумен.

§. 4. За всички неуредени в настоящите Вътрешни правила въпроси, са приложими разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни, както и действащото приложимо законодателство, което регламентира обработката на лични данни.

§. 5. Настоящите Вътрешни правила влизат в сила от датата на тяхното утвърждаването от директора на РЗИ - Шумен.

§. 6. Настоящите Вътрешни правила се преглеждат и актуализират при всяка промяна в нормативната уредба, но най- малко веднъж годишно.

ПРИЛОЖЕНИЯ:

1. Декларация за съгласие по образец **(Приложение № 1);**
2. Декларация за оттегляне на съгласие **(Приложение № 2);**
3. 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 **(Приложение №3.1);**
4. Съобщение за поверителност на кандидатите за работа **(Приложение №3.2);**
5. Съобщение за поверителност на личните данни при приемане на жалби, сигнали и предложения на гражданите**(Приложение №3.3);**
6. Съобщение за поверителност на личните данни, създадени чрез системата за видеонаблюдение на РЗИ - Шумен **(Приложение №3.4)**;
7. Съобщение за поверителност на личните данни при изпълнение на законови задължения **(Приложение №3.5);**
8. Вътрешни правила/Политика за съхранение на лични данни **(Приложение №4);**
9. Технически и организационни мерки за защита на личните данни **(Приложение №5)**

10. Споразумение за конфиденциалност за обработваните лични данни от служители и лица, наети по граждански договор (***Приложение №5.1***);

11. Споразумение за конфиденциалност за обработваните лични данни от договорни партньори на РЗИ - Шумен (***Приложение №5.2***);

12. Процедура за действие при нарушение на сигурността на личните данни (**Приложение № 6)**;

13. Процедура за упражняване на права от субектите на данните (**Приложение № 7);**

14. Споразумение за обработване на лични данни (**Приложение №8);**

15. Процедура за създаване и поддържане на регистър на дейностите по обработка на личните данни (**Приложение №9);**

16. Методика за оценка за оценка на риска, съгласно изискванията на стандарта ISO 31000 (**Приложение №10);**

17. План за действие, който съдържа необходимите механизми за контрол, отговорните лица и сроковете за изпълнение (**Приложение № 11);**

18. Процедурата за извършване на оценка на въздействието върху личните данни (**Приложение № 12);**

19. Правила за обработване, съхранение и защита на лични данни при видеонаблюдение в сградата на РЗИ - Шумен (**Приложение № 13);**

20. Процедура за предаване на лични данни на трети държави или международни организации (**Приложение № 14);**

21. Методика за оценка на съответствието (**Приложение № 15).**