РЕПУБЛИКА БЪЛГАРИЯ
Министерство на здравеопазването
Регионална здравна инспекция – Стара Загора

УТВЪРДИЛ ……/П/……
Д-Р НЕДЯЛКА КАБАДЖОВА
Директор на РЗИ – Стара Загора

ВЪТРЕШНИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В РЕГИОНАЛНА ЗДРАВНА ИНСПЕКЦИЯ – СТАРА ЗАГОРА

Стара Загора
2025 г.

Глава първа
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) Регионална здравна инспекция – Стара Загора наричана по-долу само „Инспекцията“, е юридическо лице, със седалище в гр. Стара Загора и адрес на управление: гр. Стара Загора, ул. „Стефан Караджа“ № 10.

(2) Като юридическо лице, Инспекцията изпълнява дейностите по осъществяване на държавната здравна политика на територията на област Стара Загора.

Чл. 2. Настоящите вътрешни правила за защита на личните данни, наричани за краткост **„Правилата“,** уреждат организацията на обработване на лични данни на служителите, лицата, наети на граждански договори, на контрагентите, както и на данни на физически лица от проверяваните обекти и обработвани от Инспекцията специални категории лични данни, в съответствие с изпълнение на основните й задължения.

Чл. 3. Целта на тези правила е установяването на ясна рамка и координираност в дейността на администрацията при събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, на лични данни от водените от РЗИ - Стара Загора регистри, за да се гарантира неприкосновеността на личността и личния живот, като се защитят физическите лица при неправомерно обработване на свързаните с тях лични данни и се регламентира правото на достъп до събираните и обработвани такива данни.

Чл. 4. (1) „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"); 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.

(2) „Обработването на лични данни“ означава 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.

(3) Обработването на лични данни се състои и в осигуряване на достъп до определена информация само за лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп.

(4) „Регистър с лични данни“ представлява всеки структуриран набор от лични данни, независимо от неговия вид и носител, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

Чл. 5. Регионална здравна инспекция – Стара Загора е Администратор на лични данни и води следните регистри:

5.1. Регистри и списъци, водени в изпълнение на дейностите на Инспекцията от дирекция Административно – правно, финансово и стопанско обслужване, съдържащи лични данни:

5.1.1. Информационна система „Единна информационна система за управление на човешките ресурси в държавната администрация“ /ЕИСУЧРДА/;

5.1.2. Регистър „Договори и лица по граждански договор“;

5.1.3. Регистър на декларациите по чл. 49 от ЗПК**;**

5.1.4. Регистър „Постъпили сигнали и предложения от физически и юридически лица“;

5.1.5. Регистър на регистрирани в РЗИ лични здравни книжки.

5.2. Регистри и списъци, водени в изпълнение на дейностите на Инспекцията от дирекция Медицински дейности, съдържащи лични данни:

5.2.1. Списък на лечебните заведения за извънболнична помощ и хосписите в област Стара Загора;

5.2.2. Списък на лечебни заведения за болнична помощ на територията на област Стара Загора;

5.2.3. Списък на лечебни заведения, извършващи дейности по Физикална и рехабилитационна медицина;

5.2.4. Списък на лечебните заведения за извънболнична помощ с регистриран втори адрес на територията на област Стара Загора;

5.2.5. Регистър на лекарите и лекарите по дентална медицина, които предписват лекарствени продукти, съдържащи наркотични вещества;

5.2.6. Програма - умрели и смъртност по причини;

5.2.7. УЕБ базиран портал за мониторинг на суицидните действия;

5.2.8. Платформа на МОН – Посещаемо и безопасно училище;

5.2.9. Регистър на лицата, практикуващи неконвенционални методи за благоприятно въздействие върху индивидуалното здраве;

5.2.10. Регистър за издадени удостоверения за регистрация на дрогерия;

5.2.11. Единна информационна система на медицинската експертиза;

5.2.12. Регистър на отсрочените медицински кадри от въоръжените сили при мобилизация;

5.3. Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Надзор на заразните болести, съдържащи лични данни:

5.3.1. Книга за регистриране на заразните болести;

5.3.2. Регистър „Досиета на обекти, подлежащи на противоепидемичен контрол“;

5.3.3. Регистър на информационната система за управление на имунизациите

5.3.4. Регистър на свидетелствата за имунизационно състояние;

5.3.5. Регистър на международните сертификати за ваксинация против жълта треска;

5.3.6. Регистър на издадените удостоверения за придобита квалификация за изпълнител на дезинфекции, дезинсекции и дератизации;

5.4. Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Обществено здраве, съдържащи лични данни:

5.4.1. Регионален регистър на обектите с обществено предназначение;

5.5. Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Лабораторни изследвания, съдържащи лични данни:

5.5.1. Регистър „Документация за лабораторни изследвания, извършени от дирекция ЛИ“;

Чл. 6 Личните данни се обработват на следните принципи:

(1) Законосъобразност, добросъвестност и прозрачност;

(2) Ограничение на целите – личните данни се събират за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели;

(3) Свеждане на данните до минимум – събират се само лични данни ограничени до необходимото във връзка с целите, за които се обработват;

(4) Точност – поддържане в актуален вид и предприемане на всички разумни мерки за гарантиране на своевременно изтриване или коригиране на неточни данни, при отчитане на целите на обработването;

(5) Ограничение на съхранението – личните данни са съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни; личните данни могат да се съхраняват 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 подходящи технически и организационни мерки с цел да бъдат гарантирани правата и свободите на физическите лица, чиито данни се обработват;

(6) Цялостност и поверителност - личните данни са обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически и/или организационни мерки.

(7) Отчетност – Администраторът носи отговорност и трябва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл. 7. Личните данни се събират за конкретни, точно определени цели, обработват се законосъобразно и добросъвестно и не могат да се обработват допълнително по начин, несъвместим с тези цели.

Чл. 8. Инспекцията 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 на лични данни. Предприеманите мерки са съобразени със съвременните технологични достижения и рисковете, свързани с естеството на данните, които трябва да бъдат защитени**.**

Глава втора
ВИДОВЕ РЕГИСТРИ.

Чл. 9. Видове регистри, водени от Регионална здравна инспекция – Стара Загора. Цели, за които се използват съхраняваните в отделните регистри лични данни:

(1) **Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Административно - правно, финансово и стопанско обслужване:**

1. Информационна система „ЕИСУЧРДА“

Регистърът съдържа лични данни на:

- служителите по трудови и служебни правоотношения

Регистърът се води на основание Закона за администрацията.

В регистъра се съдържат следните групи данни:

- физическа идентичност – име, презиме, фамилия, ЕГН, адрес, телефон, електронна поща, паспортни данни, образователна степен, допълнителна квалификация;
- данни, свързани със здравословното състояние – болничен лист, експертно решение;

Данните се събират и обработват от старши експерт в отдел АП, Д АПФСО, началника на отдел АП, Д АПФСО и директора на дирекция „Административно-правно, финансово и стопанско обслужване“ и се съхраняват на технически носител;

2. Регистър „Договори и лица по граждански договор“.

Регистърът съдържа лични данни на:

- контрагенти (изпълнител на доставки/услуги, възложител);
- лица на граждански договор;

Регистърът се води на основание Закона за счетоводството и други относими нормативни актове – Закона за задълженията и договорите, Закон за публичните финанси, Закон за данъците върху доходите на физическите лица, Данъчно-осигурителния процесуален кодекс, Кодекса за социално осигуряване;

В регистъра се съдържат следните групи данни:

- физическа идентичност – име, адрес, телефон, електронна поща;

Данните се събират и обработват от директора на дирекция „Административно-правно, финансово и стопанско обслужване“ и главния счетоводител в отдел ФСД, Д АПФСО и се съхраняват на хартиен и технически носител;

3. Регистър на декларациите по чл. 49 от ЗПК.
Регистърът съдържа лични данни на:
- персонал (лица по трудово и служебно правоотношение).
Регистърът се води на основание Закона за противодействие на корупцията
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, длъжност.
Данните се събират и обработват от старши експерт от отдел АП, Д АПФСО и се съхраняват от главен специалист в дирекция „Административно-правно, финансово и стопанско обслужване“ на хартиен и технически носител.

4. Регистър „Постъпили сигнали и предложения от физически и юридически лица”
Регистърът съдържа лични данни на:
- физически лица - жалбоподатели;
Регистърът се води на основание Административнопроцесуален кодекс, Закон за административните нарушения и наказания, Закон за здравето.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена;
Данните се събират и обработват от юрисконсулта в отдел АП, Д АПФСО на хартиен и технически носител;

5. Регистър на регистрирани в РЗИ лични здравни книжки.
Регистърът съдържа лични данни на:
- физически лица, потребители на услуги.
Регистърът се води на основание Закон за здравето и Наредба № 15/2006г. за здравните изисквания към лицата, работещи в детските заведения, специализираните институции за деца и възрастни, водоснабдителните обекти, предприятията които произвеждат или търгуват с храни, бръснарските, фризьорските и козметичните салони.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, месторабота;
Данните се събират и обработват от главните специалисти в отдел АП, Д АПФСО на хартиен и технически носител.

(2) Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Медицински дейности:
1. Досиета на лечебните заведения за извънболнична помощ и хосписите.
Досиетата съдържат лични данни на:
- лекари и лекари по дентална медицина, осъществяващи дейности по извънболнична помощ.
В досиетата се съдържат следните групи данни:
- физическа идентичност – три имена на лицата представляващи лечебното заведение, ЕГН, адрес, паспортни данни, № на диплома;
Данните се събират и обработват от гл. инспектор отдел ИПМЕ, мл. експерт отдел КМДЗИ на хартиен и технически носител.

2. Досиета на лечебни заведения за болнична помощ на територията на област Стара Загора.
Досиетата съдържат лични данни на:
- ръководителите на лечебните заведения.
В досиетата се съдържат следните групи данни:
- физическа идентичност – три имена на управителя на лечебното заведение;
Данните се събират и обработват от н-к отдел КМДЗИ, инспектор отдел КМДЗИ, гл. специалист отдел КМДЗИ на хартиен и технически носител.

3. Досиета на лечебните заведения за извънболнична помощ и хосписите с регистриран втори адрес на територията на област Стара Загора.
Досиетата съдържат лични данни на:
- лекари и лекари по дентална медицина, осъществяващи дейности по извънболнична помощ.
В досиетата се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, адрес, паспортни данни, № на диплома.
Данните се събират и обработват от гл. инспектор отдел ИПМЕ и мл. експерт отдел КМДЗИ на хартиен и технически носител.

4. Регистър на лекарите и лекарите по дентална медицина, които предписват лекарствени продукти, съдържащи наркотични вещества.
Регистърът не се актуализира, поради въвеждане на електронна рецепта.
Регистърът съдържа лични данни на:
- лекари и лекари по дентална медицина, предписващи лекарствени продукти, съдържащи наркотични вещества.
Регистърът се води на основание Закона за контрол върху наркотичните вещества и прекурсорите, Наредба 4 от 2009 г. за условията и реда за предписване и отпускане на лекарствени продукти.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, паспортни данни.
Данните се събират и обработват от гл. инспектор отдел КМДЗИ, гл. специалист отдел КМДЗИ на хартиен и технически носител.

5. УЕБ базиран портал за мониторинг на суицидните действия.
Системата съдържа лични данни на:
- физически лица предприели суицидни действия.
Платформата се води на основание Наредба №1 от 27 февруари 2013 за предоставяне на медико-статистическа информация и информация за медицинската дейност на лечебните заведения;
В портала се съдържат следните групи данни:
физическа идентичност – три имена, ЕГН или възраст, дата на раждане, възраст, професия, образование, семейно положение
- здравословни данни – причината за суицидното действие.
Данните се събират и обработват от мл. експерт отдел КМДЗИ, гл. специалист отдел КМДЗИ на технически носител.

6. Регистър на лицата, практикуващи неконвенционални методи за благоприятно въздействие върху индивидуалното здраве.
Регистърът съдържа лични данни на:
- лица, упражняващи неконвенционални методи за благоприятно въздействие върху индивидуалното здраве.
Регистърът се води на основание Закон за здравето, Наредба 7 от 2005 г. за изискванията към дейността на лицата, които упражняват неконвенционални методи за благоприятно въздействие върху индивидуалното здраве
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, адрес, паспортни данни;
Данните се събират и обработват от гл. инспектор отдел ИПМЕ, мл. експерт отдел КМДЗИ на хартиен и технически носител;

7. Регистър за издадени удостоверения за регистрация на дрогерия.
Регистърът съдържа лични данни на:
- ръководителя на дрогерията.

Регистърът се води на основание Закон за лекарствените продукти в хуманната медицина, Наредба № 29 от 9 декември 2008 г. за условията и реда за организация на работата в дрогерията.
В регистъра се съдържат следните групи данни:
- физическа идентичност на ръководителя – три имена, адрес;
Данните се събират и обработват от гл. инспектор отдел КМДЗИ, гл. специалист отдел КМДЗИ на хартиен и технически носител;

8. Единна информационна система на медицинската експертиза (ЕИСМЕ).
Системата съдържа лични данни на:
- пациенти (преминали освидетелстване и преосвидетелстване).
Системата се води на основание ПУОРОМЕРКМЕ и Наредба за медицинската експертиза.
В системата се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, паспортни данни, адрес;
- лични данни, които се отнасят до здравето.
Данните се събират и обработват от служители от отдел ИПМЕ, дирекция Медицински дейности, оторизирани за работа със системата. Данните се съхраняват на технически носител.

9. Информационна система за контрол на медицинската експертиза (ИСКМЕ).
Системата съдържа лични данни на:
- пациенти (преминали освидетелстване и преосвидетелстване).
Системата се води на основание ПУОРОМЕРКМЕ и Наредба за медицинската експертиза.
В системата се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, паспортни данни, адрес;
- лични данни, които се отнасят до здравето.
Данните се събират и обработват от служители от отдел ИПМЕ, дирекция Медицински дейности, оторизирани за работа със системата. Данните се съхраняват на технически носител.

10. Списък на отсрочените медицински кадри от въоръжените сили при мобилизация.
Списъкът съдържа лични данни на:
- медицински специалисти на територията на област Стара Загора.
Списъкът се води на основание Закон за отбраната и въоръжените сили на Р България.
В списъка се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, месторабота;
Данните се събират и обработват от главен експерт в отдел КМДЗИ, дирекция Медицински дейности на хартиен и технически носител.

(3) Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Надзор на заразните болести:

1. Книга за регистриране на заразните болести.
Регистърът съдържа лични данни на:
- пациенти;
Регистърът се води на основание Закона за здравето, Наредба №21/2005г. за регистрация, съобщаване и отчет на заразните болести, Сборник инструктивни материали за борба със заразните болести на МЗ/1985г.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена на заболелия, адрес, месторабота;

- лични данни, които се отнасят за здравето;

Данните се събират, обработват от старши специалист, инспектори, старши инспектори, главни инспектори в отдел Противоепидемичен контрол, дирекция „Надзор на заразните болести“ и се съхраняват на хартиен носител;

2. Регистър Досиета на обекти, подлежащи на противоепидемичен контрол.

Регистърът съдържа лични данни на:
- лица, подлежащи на противоепидемичен контрол;

Регистърът се води на основание Закона за здравето.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, адрес, телефон, паспортни данни;

Данните се събират, обработват от служителите в отдел „Противоепидемичен контрол“, дирекция „Надзор на заразните болести” на хартиен и технически носител. Данните се съхраняват на хартиен носител в дирекция „Надзор на заразните болести”;

3. Регистър на информационната система „БИОПРОДУКТИ“:

Регистърът съдържа лични данни на:
- деца до 18г.

Регистърът се води на основание Закона за здравето и Наредба №15/2005г. за имунизациите в Република България.
В регистъра се съдържат следните групи данни:
- физическа идентичност – име, ЕГН, адрес;

Данните се събират и обработват от инспектор, главен инспектор в отдел „Противоепидемичен контрол“, дирекция „Надзор на заразните болести” на хартиен и технически носител;

4. Регистър на свидетелствата за имунизационно състояние.

Регистърът съдържа лични данни на:
- потребители на услуги;

Регистърът се води на основание Закона за здравето, Наредба № 15/2005г. за имунизациите в Република България
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, дата на раждане, адрес;

Данните се събират и обработват от служители в отдел „Противоепидемичен контрол“ дирекция „Надзор на заразните болести” на технически и хартиен носител;

5. Регистър на издадените удостоверения за придобита квалификация за изпълнител на дезинфекции, дезинсекции и дератизации.

Регистърът съдържа личните данни на:
- физически лица, придобили удостоверение;

Регистърът се води на основание Закона за здравето, Наредба № 1/2018г за условията и реда за извършване на дезинфекции, дезинсекции и дератизации;
Регистъра съдържа следните групи лични данни:
- физическа идентичност – три имена, ЕГН, телефон за контакти;

Данните се събират и обработват от инспектор и главен инспектор в дирекция „Надзор на заразните болести“ на хартиен и технически носител.

(4) Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Обществено здраве:

1. Система за контролна дейност и проверка на обекти и продукти**.**

Регистърът съдържа лични данни на:
- потребители на услуги;

Регистърът се води на основание Закона за здравето и Наредба № 9/2005г. за условията и реда за създаване и поддържане на публичен регистър на обектите с обществено предназначение, контролирани от РЗИ.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена, ЕГН, адрес,;
Данните се събират и обработват от инспектори и главен специалист от отдел „Държавен здравен контрол“ и отдел „Здравно – техническа експертиза“, дирекция Обществено здраве на хартиен и технически носител.

(5) **Регистри, водени в изпълнение на дейностите на Инспекцията от дирекция Лабораторни изследвания:**
1. Регистър „Входящ-изходящ журнал ПУ“ на Лабораторен изпитвателен комплекс
Регистърът съдържа лични данни на:
- потребители на услуги;
Регистърът се води на основание Закона за здравето.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена и адрес.
Данните се събират, обработват и съхраняват от служители от дирекция „Лабораторни изследвания” на хартиен носител;

2. Регистър „Входящ-изходящ журнал ПУ“ на Орган за контрол от вида А
Регистърът съдържа лични данни на:
- потребители на услуги;
Регистърът се води на основание Закона за здравето.
В регистъра се съдържат следните групи данни:
- физическа идентичност – три имена и адрес.
Данните се събират, обработват и съхраняват от служители от дирекция „Лабораторни изследвания” на хартиен носител;

Чл. 10. (1) Право на достъп до регистрите с лични данни имат само оторизираните служители на Инспекцията, както и обработващи лични данни, на които Администраторът е възложил обработването на данни от съответния регистър при условията на чл. 28 от Общия регламент относно защитата на данните.

(2) Оторизирането на служители се извършва на основание длъжностна характеристика и/или чрез заповед на директора на Инспекцията.

(3) Служителите носят отговорност за осигуряване и гарантиране на регламентиран достъп до служебните помещения и опазване на регистрите, съдържащи лични данни. Всяко умишлено нарушение на правилата и ограниченията за достъп до личните данни от персонала може да бъде основание за налагане на дисциплинарни санкции по отношение на съответните работници и служители.

(4) Длъжностните лица нямат право да разпространяват информация за личните данни, станали им известни при и по повод изпълнение на служебните им задължения, което удостоверяват с подписване на декларация при постъпване на работа.

Чл. 11. Форми на водене на регистрите.

(1) Регистри, водени на хартиен носител:

1.1. Форма на организация и съхраняване на личните данни - писмена (документална), съхраняват се в папки (кадрови досиета, досиета на изпълнители и контрагенти) за всеки служител или наето по граждански договор лице, както и за всеки контрагент, с когото е сключен договор папките се съхраняват в административната сграда на РЗИ – Стара Загора, находяща се в гр. Стара Загора, ул. „Стефан Караджа“ № 10.

1.2. Местонахождение на картотечните шкафове: в седалището и адреса на Регионална здравна инспекция – Стара Загора. Кадровите досиета на служителите се съхранявате в стая № 108, а досиетата на контрагентите в метална каса в кабинета на

директора на дирекция АПФСО. Помещенията, в които се съхраняват са с ограничен достъп – заключващ механизъм, централна охрана, картотечни шкафове, метална каса;

1.3. С оглед защита на хартиените, техническите и информационните ресурси всички служители са длъжни да спазват правилата за противопожарна безопасност

(2) Регистри, водени на технически носител:

2.1. Форма на организация и съхраняване на личните данни - информацията се съхранява на компютри. Достъпът до тях е ограничен с индивидуална парола, при използване на специализирани информационни системи с ограничен достъп се използва и допълнителни средства за защита *(КЕП или друг код за автентификация)*.

2.2. Местонахождение на компютрите: Всеки компютър се намира в работното помещение на определения отговорен служител, отговарящ за достъп до съответната система. До тези помещения външни лица не се допускат.

2.3. Програмно-апаратни мерки за гарантиране нивото на сигурност .

2.3.1. РЗИ – Стара Загора разполага с локална компютърна мрежа, обхващаща всички компютърни работни станции, работещи под Windows и с инсталирани антивирусни програми. Ограничаването на достъпа до данни се осигурява от пароли за стартиране на операционната система и парола за достъп до програмната среда, на места се използват и допълнителни средства за защита като КЕП;

2.3.2. Инспекцията разполага и с 3 външни хард диска, които се използват за архивиране. Всички компютри, съдържащи електронни данни по съответните регистри са снабдени с надеждна антивирусна защита.

2.3.3. Работните станции, свързани във вътрешната мрежа са преминали през допълнително обработване - ограничаване на възможността за поставяне на USB флаш, забранени са макросите (*където е приложимо*), всички компютърни станции са ъпдейтвани с операционни системи спрямо възможностите им, интернет доставчиците са конфигурирали филтри на e-mail сървърите и има вграден spam филтър, служителите нямат право да инсталират софтуер, действието на Server Message Block protocol в Windows базирани системи е ограничено (*където е възможно*), забранен е autorun на машините, забранен е Remote Desktop Protocol, ограничен е периметърът на действие на щетите от Ransomware, посредством което е минимизиран рискът от изтичане на информация.

Глава трета
ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 12. (1) Регионална здравна инспекция – Стара Загора възлага обработването на личните данни на отговорни служители със заповед на директора. Обработването може да се възлага на повече от един отговорен служител съобразно спецификата на техните функции и с цел разграничаване на конкретните им задължения.

(2) Отговорните служители обработващи лични данни се определят с настоящите вътрешни правила, заповед на директора и длъжностните характеристики на служителите, а в случай на възлагане обработката на лични данни на трето лице – обработващ - в съответния договор сключен между него и Администратора – Приложение № 4.

(3) При постъпване на работа в Регионална здравна инспекция – Стара Загора всеки служител подписва декларация, съгласно Приложение № 3.

Чл. 13. **(1)** След постигане целта на обработване на личните данни, съдържащи се в поддържаните от Инспекцията регистри, личните данни следва да бъдат унищожени при спазване на утвърдената процедура за унищожаване на лични данни (*Приложение № 1*).

(2) В случаите, в които се налага унищожаване на носител на лични данни, Инспекцията прилага необходимите действия за заличаването на личните данни по начин, изключващ възстановяване, като:

1. Личните данни, съхранявани на електронен носител, се унищожават чрез трайно изтриване, вкл. презаписването на електронните средства или физическо унищожаване на носителите;

2. Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване.

Глава четвърта
ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ

Чл. 14. (1) РЗИ – Стара Загора обработва специални категории лични данни свързани със здравословно състояние на гражданите в област Стара Загора, само когато това задължение произтича от закон.

(2) Условията за обработване на специални категории лични данни са:

1. Обработването е необходимо за изпълнение на една или повече конкретни цели, свързани с дейността и функциите на Инспекцията, съгласно Устройствен правилник на регионалните здравни инспекции, Закон за здравето и други нормативни актове;

2. Обработването е необходимо за целите на изпълнението на задълженията и упражняването на специални права на Администратора или на субекта на данните по силата на трудовото и осигурителното право;

3. Обработването е необходимо за защита на жизненоважни интереси на субекта на данните или на друго физическо лице, когато субекта на данните физически или юридически не е в състояние да даде съгласието си;

4. Обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

5. Обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;

6. Обработването е необходимо по причини от важен обществен интерес на основание правото на ЕС 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 субектите на данните;

7. Обработването е необходимо за целите на трудовата медицина;

8.Обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статически цели съгласно чл.89, параграф 1 от ОРЗД, на основание правото на ЕС или националното законодателство.

Чл. 15. При обработването на специални категории лични данни на дете на възраст под 16 години РЗИ – Стара Загора като Администратор на лични данни полага разумни усилия, за да се установи автентичността на родителската отговорност от носещия родителската отговорност.

Глава четвърта
ЗАЩИТА НА ЛИЧНИТЕ ДАННИ. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА.

Чл. 16. Осигуряване на достъп на лицата до личните им данни:

(1) Всяко физическо лице има право на достъп до отнасящи се за него лични данни. В случаите, когато при осъществяване правото на достъп на физическото лице могат да се разкрият лични данни и за трето лице, Администраторът е длъжен да предостави на съответното физическо лице достъп до частта от тях, отнасяща се само за него.

(2) Достъп до лични данни може да бъде предоставен под формата на устна или писмена справка или на преглед на данните от съответното физическо лице или от изрично упълномощено от него друго лице.

(3) Заетите по трудови и служебни правоотношения, както и контрагентите, имат право на достъп до личните си данни, които се съхраняват в Регионална здравна инспекция – Стара Загора. За целта лицата подават писмено заявление до Инспекцията (*Приложение № 2).*

(4) Заявлението съдържа име на лицето, адрес и други данни, които го идентифицират – три имена, ЕГН, длъжност и месторабота (когато е необходимо), описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес за кореспонденция, а когато заявлението се подава от упълномощено лице и нотариално заверено пълномощно.

(5) При получаване на заявление за достъп до собствени на заявителя лични данни, директорът на Регионална здравна инспекция – Стара Загора разглежда заявлението за достъп. Срокът за разглеждане на заявлението и произнасяне по него е 30-дневен от деня на подаване на искането. Инспекцията предприема необходимите мерки за предоставяне на информация, която се отнася до обработването на лични данни на заявителя в кратка, прозрачна, разбираема и лесно достъпна форма на ясен език. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение, че идентичността на субекта на данните е доказана с други средства.

(6) Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение, което отново се съобщава на заявителя по реда на предходното изречение.

(7) Администраторът предоставя на заявителя следната информация:

7.1. Данните, които идентифицират Администратора и координатите за връзка с него;

7.2. Координатите за връзка с длъжностното лице по защита на личните данни, когато е приложимо;

7.3. Целите на обработването, за което личните данни са предназначени, както и правното основание за тяхното обработване;

7.4. Съответните категории лични данни на заявителя, които се обработват от Администратора;

7.5. Получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави по смисъла на Регламента или международни организации, както и техните гаранции за защита;

7.6. Съществуването на право да се изиска от Администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със заявителя, както и правото да се направи възражение срещу такова обработване;

7.7. Правото на жалба до Комисията за защита на личните данни.

7.8. Когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник.

(8) Администраторът се задължава да съобщава за всяко коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Чл. 17. (1) Регионална здравна инспекция – Стара Загора се задължава, в случай на постъпила молба от физическо лице, чийто лични данни се обработват от Администратора, да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:

1. Личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

2. Лицето оттегля своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;

3. Лицето възразява срещу автоматичното вземане на решения, прилагано от Администратора с неговите лични данни и няма други законни основания за

обработването, които да имат преимущество, или лицето изрично възразява срещу обработването;
4. Личните данни са били обработвани незаконосъобразно;
5. Личните данни трябва да бъдат изтрити с цел спазване на задължение по европейското или национално право;

(2) Инспекцията има право да откаже извършването на действията по ал. 1, ако обработването е необходимо:
1. За упражняването на правото на свобода на изразяването и свобода на информацията;
2. За спазване на правно задължение, което изисква обработване, предвидено в европейското или национално законодателство, което се прилага спрямо Администратора или за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на Администратора;
3. По причини от обществен интерес в областта на общественото здраве;
4. За целите на архивирането в обществен интерес, за научни изследвания или за статистически цели, доколкото съществува вероятност правото, установено в националното законодателство да направи невъзможно или сериозно да затрудни постигането на целите на това обработване;
5. За установяването, упражняването или защитата на правни претенции.

Чл. 18. Достъп на трети лица до лични данни на служители, лица по граждански договор и/или контрагенти на Регионална здравна инспекция – Стара Загора е ограничен.

(1) Носителите на лични данни не се изнасят извън сградата на Администратора и не се предоставят на трети лица освен в предвидените от закона случай.

(2) Никое трето лице няма право на достъп до личните данни на служителите, лицата по граждански договор и/или контрагентите на Регионална здравна инспекция – Стара Загора, освен ако същите не са изискани по надлежен ред от компетентни държавни органи (органи на съдебната власт, ревизиращи държавни органи и др.) в предвидените в закона случаи. На компетентните органи се осигурява достъп до личните данни съгласно законовите изисквания в зависимост от конкретния случай.

Чл. 19. (1) Предоставянето на лични данни в държава - членка на Европейския съюз, както и в друга държава - членка на Европейското икономическо пространство, се извършва при спазване на изискванията на действащото европейско и национално законодателство.

(2) Предоставяне на лични данни в трета държава извън тези по ал. 1 се допуска само ако тя осигурява адекватно ниво на защита на личните данни на своя територия.

Чл. 20. (1)Документите и преписките, подлежат на периодично архивиране.

(2) Трайното съхраняване за нуждите на архивирането на документи, съдържащи лични данни, се извършва на хартиен носител в помещения, определени за архив, за срокове, съобразени с действащото законодателство. Помещенията, определени за архив, са оборудвани с пожароизвестителни системи и пожарогасители и задължително се заключват.

(3) Документите на електронен носител се съхраняват на специализирани компютърни системи и/или външни носители на информация. Архивиране на личните данни на технически носител се извършва периодично от съответния служител изпълняващ тази функция (гл. експерт в отдел АП, дирекция АПФСО) с оглед запазване на информацията за съответните лица в актуален вид и с цел осигуряване на възможност за възстановяване, в случай на погиване на основния носител/система. Архивните копия се съхраняват на различно местоположение от мястото на компютърното оборудване, обработващо данните. Достъп до архивите имат само, определените със заповед на директора длъжностни лица.

Чл. 21. (1) В случай на нарушение на сигурността на личните данни, директорът на инспекцията, без ненужно забавяне, но не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни Комисията за защита на личните данни (КЗЛД), освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите

лица. Ако уведомлението до КЗЛД не е подадено в срок от 72 часа от нарушението, Инспекцията трябва да съобщи и причините за забавянето.

(2) Уведомлението съдържа най-малко следната информация:

1. описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

2. посочване на името и координатите за връзка с длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

3. описание на евентуалните последици от нарушението на сигурността на личните данни;

4. описание на предприетите или предложените от Администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(3) В случаите, когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни. Съобщението следва да бъде дадено на ясен и прост език, да дава информация за естеството на нарушението на сигурността на личните данни и да съдържа най-малко информация относно:

1. името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

2. евентуалните последици от нарушението на сигурността на личните данни;

3. предприетите или предложените от Администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

(4) Задължението на Инспекцията за уведомяване на субекта на личните данни по ал.3 не се прилага, в случай че е налице едно от следните условия:

1. Инспекцията е предприела подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

2. Инспекцията е взела впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

3. То би довело до непропорционални усилия на Инспекцията.

Чл. 22. Инспекцията има задължение да извърши оценка на въздействието съгласно изискванията на Регламент 679/2016 ЕС, в случай че обработваните от него лични данни биха могли да породят висок риск за правата и свободите на физическите лица. Оценка на въздействие е процес за определяне нивата на въздействие върху конкретно физическо лице или група физически лица, в зависимост от характера на обработваните лични данни и броя на засегнатите физически лица при нарушаване на поверителността, целостта или наличността на личните данни. Оценката на въздействието се извършва периодично на всеки две години, а при промяна на характера на обработваните лични данни или броя на засегнатите физически лица, оценката на въздействието може да бъде извършвана и по-често.

Чл. 23. При повишаване на нивото на чувствителност на информацията, произтичащо от изменение в нейния вид или в рисковете при обработването й, Инспекцията може да определи допълнителни мерки за защита на информацията от съответния регистър на лични данни.

Чл. 24. Със заповед № РД-01-178/21.08.2024г. на директора на РЗИ-Стара Загора е определено *длъжностно лице по защита на данните.*

Чл. 25. При изпълнение на своите функции Длъжностното лице по защита на личните данни е длъжен:

1. Да информира и съветва Администратора и служителите, които извършват обработване, за техните задължения по силата на Закона за защита на личните данни и Регламента за защита на личните данни и на други разпоредби за защитата на данни;

2. Да наблюдава спазването на Закона за защита на личните данни и Регламента за защита на личните данни и на други разпоредби за защитата на данни на равнище Съюз или държава членка и на политиките на Администратора по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване и съответните одити;

3. Да предоставя съвети по отношение на оценката на въздействието върху защитата на данните при поискване;

4. Да си сътрудничи с Комисията за защита на личните данни (КЗЛД);

5. Да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в чл. 36 от Регламента за защита на личните данни и по целесъобразност да се консултира по всякакви други въпроси;

6. Да участва в заседания на ръководството и работни групи, когато се обсъждат въпроси от областта на защитата на личните данни;

7. Да дава становище/съвет/мнение по всички въпроси, свързани със защитата на личните данни, консултира администратора на лични данни и съгласува всички изходящи документи съдържащи лични данни;

8. Да изпълнява и други задачи и задължения, свързани със защитата на личните данни, които не водят до конфликт на интереси;

9. Да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държавите членки;

10. Да уведомява администратора и субекта на данни в случай на нарушаване на сигурността на личните данни, както и документират всяко нарушение на сигурността на личните данни, в т.ч. фактите, свързани с нарушението, последиците от него, предприетите действия за справяне с нарушението. Уведомяването следва да се извърши незабавно след узнаване на нарушаването на сигурността.

Чл. 26. При изпълнение на задълженията си определеното длъжностно лице по защита на данните има следните права:

1. Да събира информация за определяне на дейностите по обработване;

2. Да анализира и проверява изпълнението на дейностите по обработване;

3. Да информира, съветва и отправя препоръки към Администратора на лични данни;

4. Да получава информация и необходимото съдействие от страна на ръководството на РЗИ - Стара Загора и от всички обработващи лични данни в Инспекцията.

Глава Пета
МЕРКИ ЗА ОСИГУРЯВАНЕ ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 27. Инспекцията прилага адекватна защита на личните данни, която включва:

1. Физическа защита;

2. Персонална защита;

3. Документална защита;

4. Защита на автоматизирани информационни системи и мрежи;

Чл. 28. Физическата защита в Инспекцията се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се извършват дейности по обработване на лични данни.

Чл. 29. Основните организационни мерки за физическа защита в Инспекцията включват:

1. определяне на помещенията, в които ще се обработват лични данни;

2. определяне на помещенията, в които ще се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;

3. определяне на организацията на физическия достъп;

(2) Като помещения, в които ще се обработват лични данни, се определят всички помещения, в които с оглед нормалното протичане на работния процес, се събират, обработват и съхраняват лични данни.

(3) Организацията на физическия достъп до помещения, в които се извършват дейности по обработка на лични данни, е базирана на ограничен физически достъп (на база заключващи системи и механизми) до зоните в обекта с ограничен достъп, включително и тези, в които са намират информационните системи. Достъп се предоставя само на служителите, на които той е необходим, за изпълнение на служебните им задължения.

(4) Всички записи и документи на хартиен носител, съдържащи лични данни, се съхраняват в заключени шкафове, които са заключени в кабинети с ограничен достъп само за упълномощен персонал.

(5) Достъпът до системите, обработващи по електронен способ лични данни, е ограничен чрез уникални потребителски идентификатори и пароли, а електронните носители са защитени по адекватен начин, в зони с контрол на достъпа.

Чл. 30. **(1).** Основните технически мерки за физическа защита в Инспекцията включват:

1. Използване на сигнално-охранителна техника;

2. Използване на ключалки и заключващи механизми;

3. Шкафове, метални каси;

4. Оборудване на помещенията с пожароизвестителни и пожарогасителни средства.

(2) Документите, съдържащи лични данни, се съхраняват в шкафове или картотеки, които могат да се заключват, като последните са разположени в зони с ограничен (контролиран) достъп. Ключ за шкафовете притежават единствено изрично упълномощените служители.

(3) Оборудването на помещенията, където се събират, обработват и съхраняват лични данни, включва: сигнално-охранителна техника, ключалки (механични или електронни) за ограничаване на достъпа единствено до оторизираните лица; заключваеми шкафове и пожарогасителни средства.

(4) Пожароизвестителните средства и пожарогасителните средства се разполагат в съответствие с изискванията на приложната нормативна уредба.

Чл. 31. (1). Основните мерки за персонална защита на личните данни, приложими в Инспекцията, са:

1. Задължение на служителите да преминат обучение и да се запознаят с нормативната уредба в областта на защитата на лични данни и настоящите Вътрешни правила Приложение № 5.

2. Забрана за споделяне на критична информация (идентификатори, пароли за достъп и др.) между персонала и всякакви други лица, които са неоторизирани;

3.Деклариране на съгласие за поемане на задължение за неразпространение на личните данни.

Чл. 32. Основните мерки за документална защита на личните данни, са:

1. Определяне на условията за обработване на лични данни - личните данни се събират и обработват само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната бизнес дейност на Инспекцията, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка и физическия носител на данните;

2. Регламентиране на достъпа до регистрите с лични *данни* – достъпът до регистрите с лични данни е ограничен и се предоставя само на упълномощени от директора служители;

3. Определяне на срокове за съхранение - личните данни се съхраняват не по-дълго от колкото е необходимо, за да се осъществи целта, за която са били събрани или до изтичане на определения в действащото законодателство срок. В Инспекцията се използва типова номенклатура на делата със срокове за съхранение.

4. Процедури за унищожаване*:* Документите, съдържащи лични данни, сроковете за съхранение на които са изтекли и не са необходими за нормалното функциониране на Инспекцията или за установяването, упражняването или защитата на правни претенции, се унищожават по подходящ и сигурен начин (*Приложение № 1*).

Чл. 33. **(1)** Защитата на автоматизираните информационни системи и/или мрежи в Инспекцията включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.(2)Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, включват:

1. Идентификация и автентификация чрез използване на уникални потребителски акаунти и пароли за всяко лице, осъществяващо достъп до мрежата и ресурсите на Инспекцията.

2. Управление на регистрите, съобразено с ограничаване на достъпа до съответния регистър единствено до лица, които са пряко натоварени и/или служебно ангажирани с неговото водене, поддръжка и обработка.

3. Защитата от зловреден софтуер.

4. Политика по създаване и поддържане на резервни копия за възстановяване.

5. Основни електронни носители на информация са: вътрешни твърди дискове (част от компютърна и/или сторидж система).

Глава шеста
ПРАВИЛА И МЕРКИ ЗА ОСИГУРЯВАНЕ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ КОМПЮТЪРНА ОБРАБОТКА

Чл. 34. **(1)** Компютърен достъп през локалната мрежа към файлове, съдържащи лични данни, се осъществява само от длъжностни лица с регламентирани права, единствено от тяхното физическо работно място, от специално определения за целта компютър и след идентификация чрез име и парола към системата. При приключване на работното време служителите изключват локалния си компютър.

(2) Инспекцията прилага адекватни мерки за технически и административен контрол, като по този начин гарантира, че само упълномощени служители получават достъп до данните за изпълнение на възложените им функции.

(3) Идентификацията на оторизираните лица за работа с лични данни задължително включва и идентификация чрез уникален потребителски акаунт, който съдържа име и парола на потребителя, права за достъп до системата и ползване на нейните ресурси.

(4) С цел повишаване сигурността на достъпа до информация служителите задължително променят използваните от тях пароли на определен от РЗИ - Стара Загора период, не по-дълъг от 6 месеца. В случай на отпадане на основанието за достъп до лични данни правата на съответните лица се преустановяват (вкл. и чрез изтриване на акаунта).

(5) Рутерите в Инспекцията позволяват да се следи интернет трафика на всички конфигурации в мрежата. Когато бъде установена нетипична активност (например влизане в нетипично време, не изключване на работна станция след изтичане на работното време и др. п.), главен експерт от дирекция АПФСО незабавно уведомява административното ръководството и длъжностното лице по защита на данните за извършване на проверка по случая.

Чл. 35. (1) В Инспекцията се използва единствено софтуер с уредени авторски права. Инсталирането и/или използването на всякакъв друг тип софтуер с неуредени авторски права е забранено.

(2) На служебните компютри се използва само софтуер, който е инсталиран от оторизирано от Ръководството на Инспекцията лице. Забранено е самоволното инсталиране на всякакъв друг вид софтуер.

Чл. 36. Служителите, на които е възложено да подписват служебна кореспонденция с квалифициран електронен подпис (КЕП), нямат право да предоставят издадения им КЕП на трети лица, респ. да споделят своя ПИН с трети лица.

Чл. 37. Настоящите вътрешни правила да се сведат до знанието на всички служители на Регионална здравна инспекция – Стара Загора.

Чл. 38. За неизпълнение на задълженията по тази вътрешни правила и действащото към съответния момент национално и европейско законодателство за защита на личните данни, съответните лица носят дисциплинарна отговорност.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящите Вътрешни Правила са разработени на основание Закона за защита на личните данни и 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.

§ 2. Настоящите вътрешни правила подлежат на актуализация и допълване.

§ 3. Вътрешните правила влизат в сила от датата на утвърждаването им със заповед на директора на РЗИ – Стара Загора.

Приложение № 1

ПРОЦЕДУРА

ЗА УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ НА ХАРТИЕН И ЕЛЕКТРОНЕН НОСИТЕЛ

ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Тази процедура описва начина и методите, посредством които РЗИ – Стара Загора осъществява унищожаването на лични данни, намиращи се на документи на хартиен и/или електронен носител, независимо дали съдържат общи или чувствителни данни и информация за физически лица, като:

- Хартиен носител означава всякакви документи на хартия, в това число оригинали, копия, документи, възпроизведени на ръка или на компютър, или печатна машина;
- Електронен носител означава всякакви средства за съхранение на информация, които могат да бъдат възпроизведени, в това число, но не само, флопи дискети, CD-R, CD-RW, DVD, магнитооптични дискове, микрофилми, видео материали и др.

Чл. 2. Процедурата е изготвена в съответствие със Закона за защита на личните данни.

Чл. 3. Процедурата цели да защити подлежащите на унищожаване лични данни от случайно изхвърляне на носителите, на които тези се намират, в общи кошчета за отпадъци и респективно от последващата им неправомерна и незаконна употреба, в това число чрез нерегламентирано възстановяване, възпроизвеждане, разпространение или използване на информацията.

Чл. 4. Подлежащите на унищожаване лични данни са били предоставени, събрани, изготвени и обработвани от РЗИ - Стара Загора. Предвидените срокове за съхранение на тези данни от конкретните регистри, към които са причислени, са изтекли и използването на данните вече не е необходимо за изпълнението на каквито и да било цели или съответното лице се е възползвало от Право на изтриване (право „да бъдеш забравен") по смисъла на чл. 17 от Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета от 27 април 2016 година.

ОПИСАНИЕ НА ПРОЦЕСА

Чл. 5. (1) Директорът на РЗИ - Стара Загора определя комисия от двама или трима служители, които ще отговорят за:

- Организирането и контролирането на действията по физическото унищожаване на документи на хартиен носител и на електронни средства, съдържащи лични данни;
- Контролирането на последващото отстраняване на отпадъците – унищожените документи/носители;
- Организирането и съгласуването на действията по предаване на хартията в пункт за рециклиране.

(2) Отговорните служители съгласно предходната алинея спазват съвместно следните практически стъпки:

(3) За хартиени носители:

- Събират документите, които подлежат на унищожаване;
- Унищожават, респективно възлагат на други служители унищожаването на хартиените документи;
- Попълват бланков протокол за извършеното унищожаване;
- Следят да не бъдат изхвърлени документи с лични данни, преди същите да бъдат унищожени;
- Следят за надеждното нарязване на документите;
- Непосредствено след унищожаването събират остатъците от документите и изхвърлят найлоновите пликове в контейнер за отпадъци или ги предават на пункт за рециклиране на хартия.

(4) За електронни носители

- Изтриват информацията, съдържаща се в електронните средства за съхранение;
- Ако изтриването на информацията, в това число на личните данни, е невъзможно, се прибягва към физическо унищожаване на електронния носител;
- След като са се уверили, че електронният носител не съдържа информация, от която могат да се извлекат лични данни, както и че изтритата информация не може да бъде възстановена, изхвърлят унищожения електронен носител в кошче за отпадъци;
- Попълват бланков протокол за извършеното унищожаване;
- Следят да не се изхвърлят електронни средства с лични данни, преди тези да са били безвъзвратно и необратимо унищожени.

Приложение № 2

ФОРМА ЗА
ЗАЯВЛЕНИЕ ОТ СУБЕКТ НА ДАННИТЕ

Информация за субекта на данни:

Данни на физическото лице.	
Три имена	
Дата на раждане	
Уникален идентификатор	
ЕГН/ЛНЧ	
Клиентски номер	
Друг	
Данни за контакт	
Държава	
Адрес за кореспонденция	
Телефонен номер	
E-mail	
Допълнителни данни за идентификация[1]	

Представител на субекта на данни:

Действате ли като представител от името на субекта на данни?	НЕ ☐ ДА ☐
Ако "Да", моля, посочете в качеството си на какъв (например родител, настойник, попечител, упълномощен представител)	
Данни на представителя:	
Три имена	
Дата на раждане	
Данни за контакт	
Държава	
Настоящ адрес	
Телефонен номер	
E-mail	
Допълнителни данни за идентификация на представителя:	*Моля, приложете доказателство*[2]*, че сте законно упълномощени да получавате тази информация.*

Вид на искането:		**Описание на искането и данни, за които се отнася**
Искане за достъп	ДА ☐	

[1] Могат да бъдат лични документи или друга информация, която недвусмислено потвърждава самоличността.
[2] Например, заверено пълномощно, удостоверение за назначаване на настойник/попечител и др.

Искане за коригиране	ДА ☐	
Искане за изтриване (право да бъдеш забравен)	ДА ☐	
Искане за ограничаване на обработването	ДА ☐	
Възражение срещу обработване	ДА ☐	
Искане за пренос на данни	ДА ☐	
Друго	ДА ☐	

2. ДЕКЛАРАЦИЯ

Аз, долуподписаният ....., като декларирам, че посочените по-горе данни са верни, с настоящото заявявам пред РЗИ - Стара Загора искането ми, посочено по-горе, относно описаните данни.

Дата: Подпис:

Аз, долуподписаният, ..., в качеството ми на представител, като декларирам, че посочените по-горе данни са верни, с настоящото заявявам пред РЗИ-СТАРА ЗАГОРА искането ми , посочено по-горе, относно описаните данни.

Дата: Подпис:

Заявявам, предпочитана форма за получаване на достъпа

☐ Лично от ЦАО
☐ Чрез лицензиран пощенски оператор
……..……..……..……...……
на адрес
.....
като декларирам, че пощенските разходи са за моя сметка, платими при получаването.
☐ По електронен път на електронна поща:
.....

Дата: Подпис:

Приложение № 3

Д Е К Л А Р А Ц И Я

Долуподписаният/-ата/ ……,
с постоянен адрес:……,
ЕГН……..заемащ/-а/ длъжността …….
……..
В РЗИ - Стара Загора, с настоящата в качеството си на длъжностно лице, чиито служебни задължения или конкретно възложена задача налагат достъп до лични данни и на основание Регламент (ЕС) 2016/679 на европейския парламент и на съвета от 27.04.2016г относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данн и за отмяна на Директива 95/46/ЕО (Общ регламен относно защитата на данните)

ДЕКЛАРИРАМ:

1. Задължавам се да не разгласявам лични данни, до които съм получил/-а/ достъп при и по повод изпълнението на служебните си задължения.
2. Известна ми е наказателната отговорност по чл. 313 от НК.

гр. Стара Загора Декларатор:.....

Дата.....г. …..……
(име, фамилия)

Приложение № 4

ДОГОВОР ЗА ОБРАБОТВАНЕ НА ДАННИ МЕЖДУ АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Администратор: **РЗИ - Стара Загора**

Днес,……., между страните:
1. **РЕГИОНАЛНА ЗДРАВНА ИНСПЕКЦИЯ – СТАРА ЗАГОРА**, със седалище и адрес на управление, гр. Стара Загора, ул. „Стефан Караджа“ № 10, идентификационен номер по БУЛСТАТ 176030488, представлявана от ……. – Директор, наричана за краткост ВЪЗЛОЖИТЕЛ, наричано в договора, АДМИНИСТРАТОР
и
2. ……,
ЕИК……. , седалище и адрес на управление…….. , представлявано от …….(ако е физическо лице се индивидуализира с ЕГН, адрес), наричано в договора, ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Дефиниции:
1. „Администратор“ на лични данни 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 ЕС или правото на държава членка, Администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на ЕС или в правото на държава членка.
2. „Обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на Администратора
3. „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

Като се има предвид че:
- АДМИНИСТРАТОРЪТ има достъп до личните данни на следните физически лица *(клиенти, служители, други)* ……..
наричани по-долу "субектите на данни", като обработването на личните данни е във връзка със следната цел: .....
- АДМИНИСТРАТОРЪТ желае ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ да извърши определени видове обработване в съответствие с настоящото споразумение.
- АДМИНИСТРАТОРЪТ е определил целта и средствата за обработване на лични данни, а именно: .....
- ОБРАБОТВАЩИЯТ ЛИЧНИ ДАННИ се е задължил да се съобрази с настоящото споразумение за обработване на данни и да спазва задълженията за сигурност и защита на лични данни съгласно Общия регламент относно защита на данните.
- АДМИНИСТРАТОРЪТ се счита за отговорна страна по смисъла на Общия регламент

Страните се споразумяха за следното:
.....

I. СРОК НА ДОГОВОРА

Чл. 1. Договорът се сключва за срок от……

II. ЦЕЛИ НА ОБРАБОТВАНЕТО

Чл. 2. Обработващият лични данни се задължава да обработва лични данни от името на Администратора в съответствие с целта и условията, определени в настоящото споразумение за обработване на данни, както следва: .....

Чл. 3. (1) Обработващият лични данни се съгласява да се въздържа от използването на личните данни за каквато и да е друга цел, различна от посочената от Администратора.

(2) Администраторът на лични данни се задължава да информира обработващия лични данни преди всяко обработване за цели, които не са предвидени в това Споразумение за обработка на данни.

Чл. 4. Обработващият лични данни обработва личните данни само по документирано нареждане на Администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това по силата на правото на ЕС или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този случай обработващият лични данни информира Администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес

III. ЗАДЪЛЖЕНИЯ НА ОБРАБОТВАЩИЯ ЛИЧНИ ДАННИ

Чл. 5. (1) Обработващият лични данни:

а) гарантира, че лицата, оправомощени от него да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

б) взема всички необходими мерки съгласно член 32 от Общия регламент във връзка със сигурността на обработването на личните данни;

в) подпомага Инспекцията да гарантира изпълнението на задълженията съгласно членове 32 - 36 от Общия регламент, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

г) по избор на РЗИ - Стара Загора заличава или връща на Инспекцията всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на ЕС или правото на държава членка не изисква тяхното съхранение;

д) осигурява достъп на Инспекцията до цялата информация, необходима за доказване на изпълнението на задълженията, и позволява и допринася за извършването на одити, включително проверки, от страна на Администратора или друг одитор, оправомощен от Инспекцията. Обработващият лични данни незабавно уведомява Администратора, ако според него дадено нареждане нарушава Общия регламент или други разпоредби на ЕС или на държавите членки относно защитата на данни;

е) спазва необходимите условия за включване на друг обработващ лични данни;

ж) подпомага Инспекцията, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задълженията му;

з) Обработващият лични данни може в рамките на настоящото споразумение да ангажира друг обработващ лични данни при следните условия ....., като гарантира, че избраният от него обработващ лични данни се е съгласил писмено със същите задължения, които са съгласувани между Инспекцията и обработващия лични данни.

и) В случай на договореност с Инспекция, обработващият може да уведоми надзорния орган за нарушения на личните данни от името на Администратора, ако Администраторът е дал на обработващия разрешение и това е част от договорните споразумения между Администратора

IV. РАЗПРЕДЕЛЕНИЕ НА ОТГОВОРНОСТТА

Чл. 6. (1) Обработващият лични данни е отговорен само за обработката на личните данни съгласно настоящото споразумение за обработка на данни, в съответствие с инструкциите на Администратора и на контролиращия орган.

(2).Обработващият лични данни гарантира, че има изрично съгласие и / или правна основа за обработка на съответните лични данни. Освен това гарантира, че съдържанието на личните данни и обработката не е незаконно и не нарушава правата на трета страна.

V. ЗАДЪЛЖЕНИЕ ЗА ДОКЛАД

Чл. 7. (1) В случай на изтичане на данни или друго нарушение съгласно Общия регламент, обработващият лични данни трябва да уведоми Инспекцията за това без забавяне, след което Администраторът информира субектите на данни и съответния надзорен орган.

(2) Във връзка с ал.1, обработващият лични данни се задължава да предостави пълна и точна информация.

(3) Обработващият лични данни се задължава да си сътрудничи със съответните органи, включително надзорни органи и / или субектите на данни, като остава отговорен за неизпълнение на законовите си задължения.

(4) Задължението за докладване включва във всеки случай задължението да докладва и фактът, че е настъпило ……..*(изтичане на данни/друго нарушение)*, включително подробности относно .....*(предполагаемата причина)*; известните и / или очаквани последствия, предложеното решение, мерките, които са предприети.

VI. СИГУРНОСТ

Чл. 8. Обработващият лични данни се задължава да предприеме подходящи технически и организационни мерки във връзка със защитата на личните данни, като .....

Чл. 9. (1) За да се потвърди спазването на настоящото споразумение за обработване на данни, Инспекцията има право да извърши одит, който има право да възложи и на независима трета страна, за което следва да уведоми писмено обработващия лични данни. Одитът може да бъде извършен при .....*(напр. конкретни основания за злоупотреба с лични данни)*, не по-рано от .....дни от ....., след като Администраторът е уведомил писмено обработващия лични данни.

(2) Констатациите по отношение на извършения одит ще бъдат обсъдени и оценени от страните.

(3) Разходите за одита ще бъдат поети от .....

VII. ИЗМЕНЕНИЕ.ПРЕКРАТЯВАНЕ

Чл. 10. (1) Настоящото Споразумение за обработване на данни се сключва за срока, посочен в

(2) Споразумението за обработване на данни може да бъде прекратено:

- с изтичане на срока;
- по взаимно съгласие, изразено писмено;
- при неизпълнение на задълженията на всяка от страните, както и при нарушения на Общия регламент, като в този случай всяка от страните има право да уведоми надзорния орган за извършеното нарушение.

Чл. 11. Настоящото споразумение за обработване на данни може да бъде изменяно само от страните по взаимно съгласие.

VIII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 12. (1) Всеки спор, възникващ между страните по отношение на и / или произтичащ от настоящото споразумение за обработване на данни, ще бъде отнесен до компетентния орган

Настоящото споразумение беше съставено в 2 екземпляра.

За Администратор..... **За Обработващ лични данни .....**

Приложение № 5

ПРОТОКОЛ

ОТ ПРОВЕДЕНО ОБУЧЕНИЕ ОТНОСНО ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ НА СЛУЖИТЕЛИТЕ В ДИРЕКЦИЯ ..... ПРИ РЗИ - СТАРА ЗАГОРА

Днес, …….. г., се проведе обучение на служители в Регионална здравна инспекция - Стара Загора на тема: Общ регламент за защита на личните данни (Регламент (ЕС) 2016/679) и Информационна сигурност. Горепосоченият/та служител/ка подробно се запознаха със същността на Регламент 2016/679, неговите основни понятия, изискванията и задълженията, които вменява. Обучението включваше и запознаване с Политиката за поверителност на Инспекцията и с установените начин и ред, по които се събират, съхраняват, архивират и се използват данните (записите) както в софтуерните системи, така и на хартиените носители (досиета).

Дата на провеждане:..... **Провел обучението:.....**

Присъствали служители:

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис

..... - **.....**
име, фамилия подпис