

ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ - БЛАГОЕВГРАД


УТВЪРДИЛ:
ДИРЕКТОР ЦСМП-БЛАГОЕВГРАД
/ Д-Р КРАСИМИР МИХАЙЛОВ/
ЗАПОВЕД № 83 / 25.05.2018 год.

П Р А В И Л А

ЗА НАЧИНА НА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ И ВОДЕНЕ НА РЕГИСТРИ ПО ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ЦСМП-БЛАГОЕВГРАД

РАЗДЕЛ I. ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. (1) ЦСМП- Благоевград е юридическо лице със седалище гр. Благоевград, Р България с основен предмет на дейност: осигуряване на своевременна спешна медицинска помощ на пострадали лица в дома, на местопроизшествието и по време на транспортирането до евентуалната им хоспитализация; осигуряване на спешен амбулаторен прием; организиране и провеждане на спешна медицинска помощ при стихийни бедствия, аварии и катастрофи на територията на региона който обслужва.

(2) Като администратор на лични данни ЦСМП- Благоевград определя целите и средствата за обработването им.

Чл. 2. (1) Настоящите правила въвеждат мерките за изпълнение и прилагане на Регламент 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г., относно защитата на физическите лица, във връзка с обработването на лични данни и относно свободното движение на такива данни.

(2) Настоящите правила уреждат организацията на обработване и защитата на лични данни на служителите, работниците и пациентите, посетителите, както и на други физически лица, свързани с осъществяването на дейността на ЦСМП- Благоевград.

Чл. 3. (1) „Обработване 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, съхраняване, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

(2) 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.

Чл. 4. ЦСМП- Благоевград е администратор на лични данни и е вписан в регистъра на администраторите на лични данни и на водените от тях регистри на личните данни с уникален идентификационен номер 22904.

Чл. 5. Правилата се приемат с цел да регламентират.

1. Създаване на процедури и механизми за гарантиране неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица от неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните;

2.Задълженията на длъжностните лица,обработващи лични данни и/или лицата които имат достъп до лични данни и работят под ръководството на администратора на лични данни, както и отговорността при неизпълнение на тези задължения.

3.Необходимите технически и организационни мерки за защита на личните данни на определените длъжностни лица от случайно или незаконно унищожаване или от случайна загуба от неправомерен достъп, изменение или разпространение, както и от други незаконни форми на обработване.

4.Видовете регистри,които се водят в ЦСМП- Благоевград и тяхното описание.

Чл. 6. (1) ЦСМП- Благоевград е лечебно заведение ,което в дейността си има достъп и обработва лични данни на физически лица/пациенти/ и служителите в ЦСМП- Благоевград.

(2) Всички действия спрямо постъпили в ЦСМП-Благоевград документи и изявления в електронен вид или на хартия се извършват при стриктно спазване на изискванията за защита на лични данни съгласно ЗЗЛД .

Чл.7. (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, он-лайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице.

(2) Защитата на лични данни се осъществява въз основа на принципи за:

- 1.Законосъобразност, добросъвестност и прозрачност.
- 2.Събиране за конкретни, изрично оказани и легитимни цели /ограничение на целите/.
3. Свеждане на данните до минимум.
4. Точни и при необходимост да бъдат в актуален вид /точност/.
5. Съхраняване във форма, която да позволява идентифицирането на субекта на данните за период не по-дълъг от необходимото за целите /ограничение на съхранението/.
6. Обработвани по начин, който гарантира подходящо ниво на сигурност /цялостност и поверителност/.

(3)Администраторът носи отговорност за спазването на т.1, т. 2 и т. 3 от ал. (2) и трябва да е в състояние да го докаже.

РАЗДЕЛ II. ВИДОВЕ РЕГИСТРИ В ЦСМП-БЛАГОЕВГРАД

Чл.8. В ЦСМП- Благоевград се водят и съхраняват следните вътрешноведомствени регистри и база данни:

1. Регистър „Персонал”.
2. Регистър „ Пациенти”.
3. Регистър „Видеонаблюдение”.

Чл. 9. **Общо описание на Регистър „Персонал” - категории лични данни и основание за обработване** /чл.20(1),т.2.от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни

(1) **Категории лични данни:**

- физическа идентичност – имена, ЕГН, адрес, паспортни данни, месторождение, телефон за връзка;
- медицински данни / карта за предварителен медицински преглед/;
- икономическа идентичност /данни относно финансовото състояние на физическото лице/.

Тези данни се предоставят от физическото лице на администратора с оглед изпълнение на съответните задължения към данъчни, осигурителни органи, банки и други институции, при което основание за обработване на тези данни е посочено в нормативен акт.

- социална идентичност/образование, номер, дата и място на издаване на дипломата/

Данните са необходими с оглед спазване нормативи или установени с платно разписание на длъжностите, изисквания за засмане респективно освобождаване на длъжности от лица.

- трудова дейност – съгласно приложените документи за трудов стаж и професионална биография.

- други / свидетелство за управление на МПС, удостоверение от КАТ за наложени наказания за допуснати нарушения на Закона за движение по пътищата, членство в селовна организация, предоставени на основание нормативно задължение/

(2) Основание за обработване

1. В регистърът се набират и съхраняват лични данни на работниците и служителите в ЦСМП-Благоевград с оглед:

- индивидуализиране на трудовите отношения съгласно Кодекса на труда.

- изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социалното осигуряване, Закон за счетоводството, Закон за облагане доходите на физическите лица, Закон за държавния архив и други.

2. Използване на събраните данни за съответните лица за служебни цели за всички дейности свързани:

- съществуване, изменение и прекратяване на трудови правоотношения;

- за изготвяне на всякакви документи на лицата, договори, допълнителни споразумения, документи удостоверяващи трудов стаж, служебни бележки, справки, удостоверения и други подобни;

- за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се за изпълнение на задълженията му по трудови договори;

- за водене на счетоводна отчетност относно възнагражденията на посочените по горе лица;

3. Всички служители на ЦСМП-Благоевград преди назначаване на работа в същия попълват декларация /Приложение № 1/ за поемане на задължение за неразпространение на лични данни, която се съхранява в досието на работника или служителя.

4. Всички кандидати за работа в ЦСМП- Благоевград попълват декларация /Приложение № 2/ за обработка и съхранение на лични данни на персонала.

Чл.10 Общо описание на Регистър „Персонал”

(1) Група регистри касаещи персонала

1. Автоматизирана информационна-комуникационна система / система 112/

2. TERES е програмен продукт обхващащ всички функции за автоматизирана обработка на информацията по персонала: трудови договори и допълнителни споразумения към тях, следене и контрол на разполагаемия отпуск, обработка на работната заплата в т.ч. обезщетения за временна негрудоспособност, отпуски, данъци, удържки и осигуровки, както и извеждане на информация, предназначена за външни системи.

3. Книга-регистър на трудови договори/допълнителни споразумения

4. Книга –регистър за трудови книжки

5. Регистър на заповедите за прекратяване на трудовите договори

6. Трудови досиета

7. Книга – регистър за ползване на платен и/или неплатен отпуск

8. Регистър на представени документи за ДОО, болнични листове /УП 2 и УП 3/

9. Кореспонденция по управление на човешките ресурси

10. Деловодна система.

11. ПП „Скипър”.

(2) Технологично описание на регистъра / чл. 20 (1), т.3 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1. Носители на данни

1.1. На хартиен носител

Съхраняват се в папки трудовите досиета за всеки работник или служител.

1.2. На технически носител

Личните данни се въвеждат на твърд диск на компютър. Достъп до личните данни е защитен с парола. При работа с данни се използват софтуерни продукти по обработка на данните относно възнагражденията на персонала, основни допълнителни възнаграждения, данъчни задължения, трудов стаж и други. Софтуерните продукти са предоставени от Министерство на здравеопазването ПП Терес и ПШ „Скипър”.

(3). Технология на обработване

Личните данни в Регистър „Персонал” се набират при постъпване на работа по трудово правоотношение на дадено лице на хартиен носител. За необходимостта от набиране на лични данни и целите, за които ще бъдат използвани, операторът на лични данни информира лицето. Обработващия лични данни –служител човешки ресурси приема заявлението/молба и придружаващите документи, които предоставя на технически сътрудник за регистриране в Деловодната система. Личните данни се предоставят на представляващия администратора на лични данни /Директор на ЦСМП-Благоевград / чрез обработващия лични данни –служител човешки ресурси на хартиен носител, с оглед преценка за годността на постъпващия да заеме съответната длъжност или за извършване на определената работа, като съгласува решението си с други длъжностни лица – завеждащ филиал, инж. ДВГ, главен счетоводител , касиер, счетоводство, икон. ТРЗ.

След одобрение на заявлението за работа от АДЛ, същото заедно с приложените към него документи, се предава на обработващия лични данни – служител, човешки ресурси и икон. ТРЗ, касиер, счетоводство за оформяне на възникването на валидно трудово правоотношение чрез изготвяне на трудов договор на технически и хартиен носител.

Изготвеният договор на техническия носител остава на отделен файл на компютъра, като достъп до него има служител, човешки ресурси, икон. ТРЗ и касиер, счетоводство. Хартиеният носител се представя за проверка законосъобразността на изготвения документ и валидизирането му чрез подписи на съответните длъжностни лица – директор, главен счетоводител, икон. ТРЗ и служител, човешки ресурси. След подписването на трудовия договор, същият заедно с останалите носители на лични данни се подрежда в трудовото /кадрово/ досие, съответно картотечен метален шкаф, а екземпляр от трудовия договор се връчва на постъпващия. При необходимост от поправка на лични данни, лицата предоставят такава на обработващият лични данни по негово искане на основание на нормативно задължение.

Чл.11 Срок за съхранение

Регистрите се съхраняват съгласно определени срокове в номенклатура на делата на ЦСМП-Благоевград , утвърдена от Държавна агенция „Архиви”, отдел „Държавен архив”- Благоевград през 2016 година.

След изтичане на срока на съхранение Постоянно действаща експертна комисия,сформирана към ЦСМП-Благоевград със заповед № 239/02.09.2016 год. на Директора на ЦСМП-Благоевград ги описва и след съгласуване с отдел „ Държавен архив”- Благоевград ги унищожават.

Регистър:съдържащ лични данни	Срок на съхранение:
1.Книга –регистър на трудови договори /допълнителни споразумения към трудовите договори	3 години
2.Книга –регистър за трудови книжки	3 години
3. Регистър на заповедите за прекратяване на трудовите договори	3 години
4.Трудови досиета	5 годиниЕК
5.Книга-регистър за ползване на платен и/или неплатен отпуск	3 години
6.Регистър на представени документи за ДОО, болнични листове	5 години

Чл.12. Предоставени услуги

Служителите и работниците в ЦСМП-Благоевград имат право на достъп само до личните си /трудови/ досиета, с цел проверка актуалността на информацията съдържаща се в тях. Достъпът до личното си досие работникът и служителя осъществява само в присъствието на обработващия лични данни.

Чл.13. Длъжности, свързани с обработване и защита на лични данни, права и задължения /чл.20(1), т.4 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1.Права на длъжностите, обработващи лични данни в ЦСМП - Благоевград

1.1.Личните данни съдържащи се в трудовите /кадрови/ досиета на персонала се обработват от служител човешки ресурси. Касиер, счетоводство при обработването относно изготвяне на разплащателни документи, свързани с преводи на възнагражденията на лицата пасти по трудови правоотношения в ЦСМП-Благоевград по банков път, достъп до операционната система съдържаща файлове за обработка на лични данни чрез индивидуална парола за отваряне на тези файлове.

1.2.Длъжностните лица, отговарящи за водене и съхранение на данните в регистъра имат право да изискват от персонала и кандидатите за работа необходимите документи.

2.Задължения, обработващи лични данни в ЦСМП - Благоевград

- да обработват личните данни законосъобразно и добросъвестно
- да използват личните данни до които имат достъп, съобразно целите за които се събират и да не ги обработват допълнително по начин, несъвместим с тези цели
- да актуализират при необходимост регистрите на лични данни
- да заличат или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите за които се обработват
- да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни се обработват.

3.Нямат право:

- да изискват от персонала допълнителни документ, неотразени в нормативно задължение
- да разпространяват информация от личните досиета и ведомостите за заплати на трети лица освен при нормативно задължение

4.За неизпълнение на задълженията по тези правила и по закона за защита на личните данни, виновното длъжностно лице се наказва с дисциплинарно наказание по Кодекса на труда, а когато е установено от надлежен орган наказанието се налага от органа по Закона за защита на лични данни;

5.При нанесени вреди на трето лице същото може да потърси отговорност по общия ред, ако стореното не представлява деяние за което се предвижда наказателна отговорност.

Чл.14.Оценка на въздействие и определяне на съответното ниво на защита /чл.20 (1), т.5 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1. „Ниско“- в случаите, когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Регистър „Персонал“	Ниво на въздействие			
	поверителност	цялостност	наличност	общо за регистъра
	ниско	ниско	ниско	ниско

2.Ниво на защита-ниско

Видове защита на личните данни:

Видове защита:	Организационни мерки
Физическа	1.Определяне на помещенията в които ще се обработват лични данни 2.Определяне на организацията на физическия достъп Технически мерки 1.Ключалки 2.Шкафове 3.Оборудване на помещенията 4.Пожарогасителни средства
Персонална	1.Познаване на нормативната уредба в областта на защита на личните данни 2.Знания за опасностите за лични данни,обработвани от администратора 3.Съгласие за поемане на задължение за неразпространение на личните данни
Документална	1.Определяне на регистрите,които ще се поддържат на хартиен носител 2.Определяне на условията за обработване на лични данни 3.Регламентиране на достъп до регистрите 4.Определяне на сроковете за съхранение 5.Процедури по унищожаване
Автоматизирани информационни системи	1.Идентификация и автентификация 2.Управление на регистрите 3.Външни връзки/свързване/ 4.Защита от вируси 5.Резервни копия за възстановяване 6.Носители на информация 7.Персонална защита 8.Определяне на сроковете за съхранение на личните данни 9.Процедури за унищожаване /заличаване/ изтриване на носители

Чл.15. **Предприети технически и организационни мерки** /чл.20 (1), т.6 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

Регистър ПЕРСОНАЛ	Физическа		Персонална	Документална	АИС
	Организационни мерки	Технически мерки	Организационни мерки	Организационни мерки	Орг.мерки
	1.Лични данни се обработват в АСС 2.Обособени помещения- 5 стая в АСС	1.Ключалки и заключване на помещенията 2.Шкафове Компютрите са поставени на бюра	Административен персонал- запознат с: 1.Наредба № 1/30.01.2013г. 2.Правила за начина на	1.Определяне на регистрите , които ще се поддържат на хартиен носител- трудови/лични /досиета, трудови	1.Достъп до системата ТЕРЕС има икон. ТРЗ, касиер, счетоводство и

	<p>3.Парола за стартиране на програмата и персонален потребителск и профил</p>	<p>и плотове</p> <p>3.Помещенията са оборудвани с изправна СОД система</p> <p>4.Пожарогасителните средства са поставени на видни места</p>	<p>обработване на лични данни и водене на регистри по ЗЗЛД в ЦСМП-Благоевград</p> <p>Заповед..... г. на директора</p> <p>3.Преди назначаване на работа всеки служител/работник в АСС попълва Декларация за конфиденциалност</p>	<p>договори и ведомости за работни заплати</p> <p>2. Условието за обработване на лични данни регламентиране достъпа до регистрите, сроковете за съхранение и процедурите за унищожаване</p>	<p>служител,човешки ресурси.</p> <p>2. Достъп до „Регистър спешни повиквания 112” икон. ТРЗ, главна медицинска сестра и технически сътрудник и.</p> <p>3.Системата „Регистър спешни повиквания 112” е изолирана от интернет</p> <p>4.Софтуера е защитен от вируси</p> <p>5.База данни с на национално ниво</p>
--	--	--	---	---	--

Чл.16. Действия за защита при аварии, произшествия и бедствия/ пожар,наводнения и други/чл.20(1),т.7 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/ . Съблюдават се всички необходими мерки за предотвратяване на:

- наводнения от водопроводната мрежа или парно отопление
- пожар

При реално настъпило бедствие или авария регистрите на хартиен посетител се пренасят в незасегнатите помещения/регистрите са в работни помещения,поставени на работни плотове и/или бюра,високо от земята/. Комютърните конфигурации в АСС на ЦСМП-Благоевград са поставени на висок работен плот/бюра.

Чл.17.Предоставяне на лични данни на трети лица-основание, цел, категории лични данни / чл.20(1),т.8 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

(1) Информация по личните данни може да бъде предоставена на трети лица /Заявление – Приложение № 4/:

(2) Трудовото досие на лицето не се изнася извън сградата на администратора

(3)Никое длъжностно или трето лице няма право на достъп до трудовите досиета на персонала на ЦСМП-Благоевград, освен ако същото е изискано по надлежен ред от органи на съдебната власт, съд, прокуратура, следствени органи и полиция; НОИ; НАП; Инспекцията по труда; достъпът на тези органи до личните данни на лицата е правомерен

(4)Надлежен е начинът при който съответния съдебен орган е изискал трудовото/кадровото/ досие или данни, съдържащи се в него, писмено с изрично искане отправено до директора на ЦСМП-Благоевград; подобни случаи на органите на съдебната власт или полицията се предоставя копие от съдържащите се от кадровото досие документи, заверени с подпис на оператора на лични данни и печат на ЦСМП-Благоевград; за идентичността на предоставените копия от документи с оригиналите им отговорност носи операторът; в

подобни случаи и ако в писменото искане на съдебния орган или полицията не се съдържа изрична забрана за разгласяване, операторът на лични данни е длъжен да информира лицето, но не и да възпрепятства работата на органите на съдебната власт или полицията;

(5) Не се изисква съгласие на лицето ако обработването на неговите лични данни се извършва само или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, административни нарушения и на непозволените увреждания; на такива лица се осигурява достъп до лични данни, като при необходимост им се осигуряват съответни условия за работа помещения на ЦСМП-Благоевград;

(6) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирани със съответни документи- писмени разпореждания на съответния орган, в който се посочва основанието, имената на лицата, като за целите на дейността им е необходимо да се осигури достъп до кадровите досиета на персонала;

(7) правомерен е достъпа на служба по трудова медицина /СГМ/с която ЦСМП-Благоевград има сключен договор за обслужване; осигурява се достъп до личните данни на нормативно основание/ Закон за здравословни и безопасни условия на труд/, проследяване здравното състояние на работниците и служителите, като при необходимост им се осигуряват съответни условия за работа в помещенията на ЦСМП-Благоевград;

Чл.18.Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните, както и за заличаването им/чл.20(1),т.9 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

Периодични прегледи се извършват при необходимост:

- промяна в нормативната база
- отпадане или възлагане на нови дейности
- промяна в организацията на работа

Чл.19.Определяне на ред за изпълнение на задълженията по чл.25 от Закона за личните данни /чл.20(1),т.10 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

(1) При промяна в статута на ЦСМП/преобразуване,ликвидация и други/ палагати прехвърляне на регистрите за лични данни от ЦСМП на друг администратор на лични данни,предаването на регистъра се извършва с разрешение на Комисията за защита на личните данни и съгласно посочения ред за внасяне на съответното искане;

(2) След постигане целта на обработване на лични данни или преди преустановяване на обработването на личните данни администратора е длъжен да ги унищожи или прехвърли на друг администратор, като предварително уведоми за това комисията, ако прехвърлянето е предвидено в закон или е налице идентичност на целите на обработването.

(3) В случаите, когато се палага унищожаване на носител на лични данни, ЦСМП-Благоевград прилага необходимите действия за тяхното заличаване по начин, изключващ възстановяване данните и злоупотреба с тях.

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

(5)Документите на хартиен носител, съдържащи данни, се унищожават чрез нарязване. Унищожаване се осъществява от служителя, отговорен за архива на ЦСМП- Благоевград или от назначена комисия, като за целта се изготвя протокол.

Чл. 20. Общо описание на Регистър„Пациенти”-категории лични данни и основание за обработване/чл.20(1),т.2.от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

(1) Категории лични данни:

1. физическа идентичност – имена, ЕГН, адрес, пол;
2. специални-чувствителни медицински данни –анамнеза, резултати от прегледа, диагноза, лечение и резултати;

(2) Личните данни на пациентите, обслужвани от ЦСМП – Благоевград се попълват в:

формуляр по образец;/Фии за СМП, Книга за повиквания от тел.112, Амбулаторна книга, Реанимационен лист, Книга за алкохолни проби, Книга за съобщения за смърт, Книга за ПТП/

(3) Основание за обработване:

1. В регистрите се събират и съхраняват лични данни за обслужени пациенти в ЦСМП-Благоевград - филиал Благоевград, Сандански, Петрич, Гоце Делчев, Разлог, Симитли, Кресна, Банско, Якоруда и Сатовча с оглед изпълнение на нормативните изисквания на Закона за здравето, Закон за лечебните заведения, Закон за движение по пътищата, Наредба №25/1999 г. за оказване на спешна медицинска помощ, Медицински стандарт „Спешна медицина” ,Правилник за устройството и дейността на център за спешна медицинска помощ, Правилник за вътрешния трудов ред на ЦСМП- Благоевград, Етичен кодекс за поведение на работниците и служителите в ЦСМП- Благоевград и други.

2. Събраните данни се използват за служебни цели:

2.1.Регистриране на пациенти,потърсили медицинска помощ на тел.:112,сами потърсили медицинска помощ или осъществен спешен транспорт на спешен пациент,манипулации,консултации,изследвания,хоспитализирани пациенти,вземане на биологичен материал за изследване на алкохол и/или наркотични вещества, при констатиране на смърт -издаване съобщение за смърт от спешните мобилни и стационарни екипи.

2.2.Регистриране на пострадалите и/или участници в ПТП

2.3.Заявка за доставка на кръв и кръвни продукти

2.4. Регистриране на вторичен транспорт на пациенти между лечебните заведения

2.5.Обработка на обобщена статистическа информация за дейността на ЦСМП- Благоевград и разкритите филиали на територията на обслужваната област, настъпили произшествия и извънредни обстоятелства.

3. Всички пациенти дават информирано съгласие преди обработването на личните им данни в първия възможен момент, в зависимост от здравословното им състояние. За деца до 14 – годишна възраст информирано съгласие се дава от родител или настойник. /Приложение 3/.

Чл.21.Общо описание на Регистър,„Пациенти”

(1) Група регистри касаещи пациента:

1.Автоматизирана информационна-комуникационна система-Районен център 112 София.

2.Приложения на Наредба № 25 за оказване на спешна медицинска помощ от 04.10.1999 год.на Министерство на здравеопазването,изм.ДВ бр.18/04.03.2014 год.:

2.1.,„Фии за спешна медицинска помощ”

2.2.,„Фии за спешна заявка”

2.3.,„Реанимационен лист”

3. Амбулаторна книга

4. Книга за повиквания и посещения на екипите на адрес

5. Книга за ПТП -регистрирани пациенти, пострадали при ПТП

6. Книга за алкохолни проби -Дневник-регистриране на взети биологични проби за употребата на алкохол и/или наркотични вещества или техните анализи на основание Наредба № 1 от 19 07.2017 год. за реда за установяване употребата на алкохол и/или наркотични вещества или техните анализи,изд. от Министерство на здравеопазването,Министерството на вътрешните работи и Министерство на правосъдието.

7. Книга за вторичен транспорт на пациенти между лечебни заведения

8.Книга за упойващи лекарствени продукти-Дневник-регистър на изразходваните лекарствени средства,съдържащи наркотични вещества , движението и отчитането на разхода по пациенти, на основание Закон за контрол върху наркотичните вещества и прекурсорите, обн.ДВ 30/02.04.1999 год.,изм. ДВ бр.17/23.02.2018 год.

9. Книга –съобщение за смърт - Регистър на издадените съобщения за смърт от спешните мобилни и стационарни екипи на основание Наредба 14/2004 год.за медицинските критерии и реда за установяване на смърт,ДВ бр.32/02.04.2013 год. на Министерството на здравеопазването.

Чл.22. **Технологично описание на регистър „Пациенти“**/ чл.20(1),т.3.от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1.Носители на данни

1.1. На хартиен носител

Форма на организация и съхраняване на лични данни-писмена,съхранява се в работните помещения – РКЦ, диспечерска зала, амбулаторни кабинети на съответния филиал/ се съхранява медицинската документация. Достъпът до регистър „Пациенти“ с ограничен - само медицинския персонал. След изписване на регистрите завеждащ ФСМП ги съхраняват в заключено помещение с достъп само от завеждащ ФСМП до предаването им в централния архив на ЦСМП - Благоевград.

Предоставяне на лични данните за пациентите става чрез устен разговор с пациента или техния придружител.

1.2.На технически носител

Форма на организация и съхраняване на лични данни - само данните в регистър автоматизирана- информационна система „информационна система за спешни повиквания“ се въвеждат от дежурните диспечери в РКЦ Благоевград. Достъп до „ информационна система за спешни повиквания“ имат работещите стационарни екипи на ЦСМП-Благоевград, който се осъществява с индивидуален потребителски профил. Софтуерните продукти са предоставени от Министерството на здравеопазването.

Местонахождението на компютрите - в помещение за работа на дежурните диспечери в РКЦ и диспечерни зали на ФСМП.

2.Технология на обработване

2.1. Личните данни в регистрите се набират при обслужване на пациентите при домашно повикване и/или амбулаторен преглед чрез устен разговор с пациента или негов придружител. Медицинският преглед се осъществява след информирано съгласие на пациента **Приложение 3/**. Регламентирано със заповед № 164/23.06.2016 г. год. на Директорът на ЦСМП- Благоевград -информирано съгласие за медицинските дейности, включително и хирургични интервенции, инвазивни и други диагностични и терапевтични дейности с повишен риск за живота и здравето и утвърдени със Заповед № 201/30.12.2015 г на Директора на ЦСМП – Благоевград **Правила за спазване правата на пациента и за предоставяне по достъпен начин на информация на пациента.**

2.2.Информираното съгласие на пациента се удостоверява срещу подпис в Декларация за информирано съгласие: **Декларация за информирано съгласие на пациента Приложение 3/**.

2.3.Медицинските дейности могат да бъдат извършвани без писмено информирано съгласие само когато са в полза на пациента и когато непосредствено е застрашен живота му и физическото или психическото му състояние не позволяват изразяване на информирано съгласие или е невъзможно да се получи такова от родственик,пастойник или попечител на лицето/чл.87(1),ал.5,ал.6, чл.88(1) и чл.162,ал.3 от Закона за здравето.

Чл. 23.Срок за съхранение

Регистрите се съхраняват съгласно определени срокове в номенклатура на делата на ЦСМП-Благоевград , утвърдена от Държавна агенция„Архиви”, отдел „Държавен архив”-Благоевград през 2016 година от завеждащ ФСМП в заключени шкафове до предаването им в централен архив на ЦСМП – Благоевград.

След изтичане на срока на съхранение Постоянно действаща експертна комисия,сформирана към ЦСМП-Благоевград със заповед № 239/02.09.2016 год. на Директора на ЦСМП-Благоевград ги описва и след съгласуване с отдел „ Държавен архив”-Благоевград ги унищожава.

Регистър:съдържащ лични данни	Срок на съхранение:
Фиш за спешна медицинска помощ	3 години
Фиш за спешна заявка	3 години
Реанимационен лист	3 години
Книга за повиквания и посещения	5 години
Амбулаторен дневник на ФСМП	5 години
Книга за Регистрирани ПТП	5 години
Книга за взети проби за алкохол	5 години
Книга за вторичен транспорт	5 години
Книга за упойващи лекарствени продукти	5 години
Книга - съобщения за смърт	5 години

Чл. 24. Предоставени услуги

Осигуряване на достъп на лицата до личните им данни

1. На основание чл.28б от Закона за здравето пациентът има право да получи от ЦСМП – Благоевград здравна информация, отнасяща се до неговото здравословно състояние, включително копия от медицинските си документи.

2. Пациентът има право да упълномощи писмено друго лице да се запознае с медицинските му документи, както и да направи копия от тях.

3. При смърт на пациента неговите наследници и роднини по права и по съребрена линия до четвърта степен включително имат право да се запознаят със здравната информация за починалия, както и да направят копия от медицинските му документи след представяне на „Удостоверение за наследници“.

4. Пациентите подават писмено заявление до Директора на ЦСМП- Благоевград /Приложение № 4/. Заявлението е безплатно, съдържа име на лицето и други данни, които го идентифицират, описание на искането, предпочитана форма за предоставяне на достъп до лични данни, подпис, адрес за обратна връзка, заверено нотариално пълномощно/когато молбата се подава от упълномощено лице/.

5. Ако при осъществяване достъп до лични данни по искане на едно лице е възможно да се разкрият лични данни за друго лице, администраторът е длъжен да предостави достъп само до частта от тях, отнасяща се до заинтересованото лице.

6. Достъп до данните на лицето се осигурява под формата на:

- устна информация
- писмена справка
- преглед на данните от самото лице от изрично упълномощено от него лице
- предоставяне на заверено копие от исканата информация
- предоставяне на копие от исканата информация на предпочитан носител, освен в случаите, когато законът забранява.

Чл.25. Длъжности, свързани с обработване и защита на лични данни, права и задължения/чл.20(1),т.4 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

(1) Оператор обработващ лични данни на регистър „Пациенти“:

-дежурен медицински персонал на смяна /лекар, фелдшер и/или медицинска сестра/ по утвърден от Директора на ЦСМП- Благоевград месечен график

-главна медицинска сестра

- завеждащи ФСМП

- технически сътрудник

1.Права

1.1. Достъп до операционната система/КИС/, съдържаща файлове с лични данни имат само: дежурни диспечери в РКЦ – Благоевград, главна медицинска сестра, служител „човешки ресурси“, икон. ТРЗ, ипж. ДВГ, технически сътрудник чрез потребителски профил за отваряне на тези файлове и индивидуална парола.

1.2. Достъп до личните данни на хартиен носител имат спешните мобилни и стационарни екипи на смяна в ЦСМП- Благоевград, завеждащ ФСМП, главна медицинска сестра и технически сътрудник.

2.Задължения

2.1. Служителите, обработващи лични данни на пациентите да спазват стриктно Правилата за защита на обработване на лични данни в ЦСМП- Благоевград. При неспазване Правилата виновното лице се наказва с дисциплинарно наказание по Кодекса на труда

2.2. Когато неизпълнението на съответното задължение е констатирано и установено от надлежен орган, наказанието се налага от органа по Закон за защита на личните данни

2.3. Ако в резултат действията на виновното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице,същото може да потърси отговорност по общия ред,ако стореното не представлява деяние за което се предвижда наказателна отговорност

(2).Оценка и ниво на въздействие, ниво на защита на основание Наредба № 1 /30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни

Чл. 26. **Оценка на въздействие и определяне на съответното ниво на защита** /чл.20(1),т.5 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1. „Средно”- в случаите,когато неправомерното обработване на лични данни би застрашило неприкосновеността на личността и личния живот на отделно физическо лице или група физически лица.

Регистър	Ниво на въздействие			
	поверителност	цялостност	наличност	общо за регистъра
Пациенти	средно	средно	средно	средно

2.Ниво на защита-средно

Видове защита на личните данни:

Видове защита:	Организационни мерки
Физическа	1.Определяне на зоните с контролиран достъп 2.Определяне на помещенията, в които ще се обработват лични данни 3.Определяне на помещенията в които ще се разполагат елементите на КИС за обработване на данни 4.Определяне на организацията на физическия достъп 5. Определяне на използваните технически средства за физическа защита Технически мерки 1.Ключалки 2.Шкафове 3.Оборудване на помещенията 4.Пожарогасителни средства
Персонална	1.Познаване на нормативната уредба в областта на защита на личните данни 2. Познаване на политиката и ръководствата за защита на лични данни 2.Знания за опасностите за лични данни,обработвани от администратора 4. Споделяне на критична информация на персонала /пароли за достъп и др./ 5.Съгласие за поемане на задължение за неразпространение на личните данни

	6. Обучение 7. Тренировка на персонала за реакция при събития, застрашаващи сигурността на данните
Документална	1.Определяне на регистрите, които ще се поддържат на хартиен носител 2.Определяне на условията за обработване на лични данни 3.Регламентиране на достъп до регистрите 4. Контрол на достъпа до регистрите 5.Определяне на сроковете за съхранение 6.Правила за размножаване и разпространение 5.Процедури по унищожаване
Автоматизирани информационни системи	1.Идентификация и автентификация 2.Управление на регистрите 3.Външни връзки/свързване/ 4. Телекомуникации и отдалечен достъп 5.Защита от вируси 6. Поддържане/експлоатация 7.Копия/Резервни копия за възстановяване 8.Носители на информация 9.Физическа среда/обкръжение 10.Персонална защита 11.Определяне на сроковете за съхранение на личните данни 12.Процедури за унищожаване/заличаване/изтриване на носители
Криптографска защита	1.Стандартните криптографски възможности на операционните системи 2.Стандартните криптографски възможности на системите за управление на бази данни 3.Стандартните криптографски възможности на комуникационното оборудване

Чл. 27. **Предприети технически и организационни мерки/чл.20(1),т.6 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/**

Регистър	Физическа		Персонална	Документална	АИС	Криптографска защита
	Организационни мерки	Технически мерки	Организационни мерки	Организационни мерки	Орг.мерки	
АИКС Автоматизирана информационно-комуникационна система	1.Лични данни се обработват в РКЦ 2.Обособени помещения-РКЦ 3.РКЦ-парола за стартиране на програмата и персонален потребителски профил	1.Ключалки денонощен режим на работа не позволява заключване на помещенията 2.Шкафове Компютрите са поставени на бюра и плотове 3.Помещенията са оборудвани	Медицинския персонал- запознат с: 1.Наредба № 1от30.01.2013г. 2.Правила за начина на обработване на лични данни и водене на регистри по ЗЗЛД в ЦСМП-Благоевград Заповед..... г. на директора	1.Регистрите на Автоматизирана информационно-комуникационна система се поддържат само на електронен носител 2. Засилване контролът на достъп до	1.Мед.специалист и работят по утвърден месечен график от директор а,в системат а влизат със собствен

		с изправна система 4.Пожарогасителните средства са поставени на видни места	3.Преди назначаване на работа всеки медицински специалист попълва Декларация за конфиденциалност и Декларация – съгласие за обработване на лични данни	регистрите 3. Определяне срокове за съхранение на информацията 4. Изготвяне Процедура за унищожаване	и пароли. 2.Имат достъп само в системата на „Регистър спешни повиквания 112“ 3.Системата е изолирана от интернет 4.База данни е на национално ниво 5.Обработва се информацията постъпила от Районен център 112 София
Медицинска документация, съдържаща лични данни на пациенти на хартиен носител	1.Личните данни се обработват от дежурния медицински персонал при изпълнение на домашните повиквания и амбулаторните прегледи във ФСМП - Сандански, Петрич, Симитли, Кресна, Банско, Разлог, Якоруда, Гоце Делчев и Сатовча 2.Физически достъп се осъществява от дежурен медицински персонал по утвърден месечен график	1.Осигуряване на индивидуални ключалки и заключване на обособените помещения. 2. Наличие на заключващи се шкафове за съхранение на документи 3.Наличие на изправни пожарогасителните средства във ФСМП 4.Оборудване на зоните с контролиран достъп/метални решетки/	Запознаване на медицински персонал с: 1.Правила за начина на обработване на лични данни и водене на регистри по ЗЗЛД в ЦСМП-Благоевград 2. Декларацията за информирано съгласие за обработване на лични данни на пациентите 3. Провеждане на обучение за прилагане на регламент 2016/679 4.Провеждане на тренировка за реакция при събития, застрашаващи сигурността на	1. Определяне на регистрите за обработка на лични данни 2. Осъществяване на контрол на достъп до регистрите.	

от директора	данните			
--------------	---------	--	--	--

Чл. 28. Действия за защита при аварии, произшествия и бедствия/ пожар, наводнения и други/чл.20(1),т.7 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/ Съблюдават се всички необходими мерки за предотвратяване на:наводнения от водопроводната мрежа или парно отопление, пожар. При реално настъпило бедствие или авария регистрите на хартиен носител се пренасят в незасегнатите помещения/регистрите са в работни помещения,поставени на работни плотове и/или бюра,високо от земята/. Компютрите в РКЦ са поставени на висок работен плот.

Чл. 29. Предоставяне на лични данни на трети лица-основание,цел,категории лични данни / чл.20(1),т.8 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1. Медицинските регистри и цялата медицинска документация не се изнасят извън сградите на филиалите и административно-столовски сектор на ЦСМП-Благоевград

2. Право на достъп до медицинската документация на ЦСМП- Благоевград държавните органи на МВР, съд, прокуратура, следствие и други, изискани по надлежен ред във връзка с изпълнението на техните правомощия.

3. Органът изискал медицинската документация или данни,съдържащи се в нея отправя писмено искане до Директора на ЦСМП- Благоевград. В тези случаи на искащият орган се изпраща писмо с обратна разписка и/или лично срещу подпис.

-Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, административни нарушения и непозволенни увреждания

-На представителите на компетентни държавни органи се осигурява достъп до лични данни

4. При промяна в статута на ЦСМП-преобразуване, ликвидация и други, налагащи прехвърляне на регистрите за лични данни от ЦСМП на друг администратор на лични данни, предаването на регистъра се извършва с разрешение на Комисията за защита на личните данни и съгласно посочения ред за внасяне на съответното искане.

Чл. 30. Срок за провеждане на периодични прегледи относно необходимостта от обработване на данните,както и за заличаването им/чл.20(1),т.9 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/ Периодични прегледи се извършват при необходимост:

1.промяна в нормативната база

2.отпадане или възлагане на нови дейности

3.промяна в организацията на работа

Чл. 31. Определяне на ред за изпълнение на задълженията по чл.25 от Закона за личните данни/чл.20(1),т.10 от Наредба № 1 от 30.01.2013 год. за минималното ниво на технически и организационни мерки и допустимия вид на защита на личните данни/

1.при промяна в статута на ЦСМП/преобразуване,ликвидация и други/ налагащи прехвърляне на регистрите за лични данни от ЦСМП на друг администратор на лични данни,предаването на регистъра се извършва с разрешение на Комисията за защита на личните данни и съгласно посочения ред за внасяне на съответното искане

2.след постигане целта на обработване на лични данни или преди преустановяване на обработването на личните данни администратора е длъжен да ги унищожи или прехвърли на друг администратор,като предварително уведоми за това комисията,ако прехвърлянето с предвидено в закон или е налице идентичност на целите на обработването.

Чл. 32 (1) Общо описание на регистър „Видеонаблюдение“ се набират и съхраняват лични данни с цел индивидуализиране на физически лица, съгласно Закона за частната охранителна дейност.

(2) Общо описание на регистър „Видеонаблюдение“:

Категориите физически лица, за които се обработват лични данни, са посетители, пациенти, придружители и служители в сградите на ЦСМП- Благоевград.

Регистърът съдържа следните групи данни - физическата идентичност на лицето – видеообраз.

(3) Технологично описание на регистър „Видеонаблюдение“: Регистърът се попълва с данни от автоматично денонощно видеонаблюдение (видеообраз) за движението на служителите и посетителите в сградите на ЦСМП- Благоевград.

(4) Определяне на длъжностите: Оператори на лични данни на регистър „Видеонаблюдение“ са фирма „ЕЛОС“ ООД.

(5) Нивото на въздействие на регистъра по отношение на различните критерии е, както следва:

1. поверителност – ниско ниво;
2. цялостност – ниско ниво;
3. наличност – ниско ниво;
4. общо за регистъра – ниско ниво.

(6) Организационни мерки за физическа защита – определени помещенията, в които се обработват лични данни, като физическия достъп е ограничен само за служители с оглед изпълнение на служебните им задължения.

(7) На входовете и вътре в сградата са поставени информационни табели за уведомяване на служителите, пациентите и гражданите, че са под видеонаблюдение, съгласно ЗЧОД и за използването на техническите средства за наблюдение и контрол.

(8) Категориите лица, на които личните данни могат да бъдат разкривани са физическите лица, за които се отнасят данните, и на лица, ако е предвидено в нормативен акт.

(9) Лични данни се съхраняват в паметта на дивира за срок от 15 дни. При необходимост записите могат да бъдат свалени на външен носител.

(10) След постигане целите по предходната алинея личните данни се унищожават физически, чрез изтриване.

(11) Данните в регистъра се предоставят доброволно от лицата при подхода и влизането им в сградите на ЦСМП- Благоевград.

РАЗДЕЛ III. ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ В ЦСМП - БЛАГОЕВГРАД

Чл.33 (1) Директорът на ЦСМП – Благоевград възлага обработването на лични данни на служители на ЦСМП- Благоевград, съобразно спецификата на изпълняваните от тях служебни функции/оторизиран достъп само до тези регистри и база данни, които са необходими за изпълняване на техните служебни задължения/

(2) Предоставянето, промяната или прекратяването на оторизиран достъп до база данни се конкретизира от Директора на ЦСМП - Благоевград.

Чл.34 Директорът на ЦСМП- Благоевград осъществява контрол върху законосъобразното водене, поддържане и обработване на личните данни в регистрите и базите данни.

Чл.35(1) Лицата подават личните си данни до АЛД чрез длъжностното лице /служител „Човешки ресурси“ – за регистър „Персонал“, дежурен медицински екип – за регистър „Пациенти“/

(2) Обработващият данните информира техния притежател, относно необходимостта от набирането им и целите, за които ще бъдат използвани.

(3) Носител(форма) за предоставяне на данните от физическите лица-личните данни за всяко лице се набират в изпълнение на нормативно задължение чрез:

- писмени документи/хартиен носител/
- електронен носител
- технически носител

-външни източници в изпълнение на нормативни изисквания

Чл.36. При въвеждане, промяна или предаване на лични данни в базите данни, администраторът осигурява съхраняване на информация за:

- времето/дата и час/ на въвеждане, промяна на личните данни
- лицата, извършващи въвеждането, промяната или предаването на лични данни

- лицата, предоставили личните данни

- промените или предадени лични данни, които са била въведени

Чл.37(1). Личните данни, организирани върху хартиен носител се съхраняват в папки /в шкафове/ в кабинетите на съответните служители, които извън работно време се заключват.

(2). Личните данни върху технически носител се съхраняват в сървърви в помещения, които извън работно време се заключват.

(3). Личните данни не се изнасят извън сградите на ЦСМП- Благоевград.

Чл.38(1). Личните трудови досиета на служителите в ЦСМП- Благоевград, се обработват и съхраняват в АСС.

(2). Трудовите досиета се съхраняват съгласно нормативно определени срокове.

Чл.39(1). Информацията, която съдържа трудовото досие е конфиденциална и не може да бъде разгласявана без изричното писмено съгласие на работника или служителя.

(2). Личните трудови досиета имат следните нива на защита:

1. При ниско ниво на защита за лични данни, обработвани на хартиен носител, формата на организация и съхраняване на лични данни е писмена/документална/.

- трудовите досиета за всеки служител се съхраняват в папки, които се поставят в картотечен шкаф със заключване

- картотечния шкаф се намира в общо работното помещение, където се помещава служител „човешки ресурси”, поради невъзможност да се осигури самостоятелно помещение

- след приключване на работа по тях служител „човешки ресурси” заключва картотечния шкаф

2. При средно ниво на защита /за лични данни, обработвани на технически носител, в компютърна система на локален компютър или в мрежа, не свързани с обществената мрежа/ формата на организация и съхраняване на лични данни е въвеждането им на твърд диск, на отделни компютри, които са свързани с локална мрежа, но със защитен достъп на лични данни, който е непосредствен само от страна на обработващия лични данни.

Чл.40(1). При работа с данните се използват съответните софтуерни продукти за обработка на същите, включително относно управлението на човешки ресурси, възнагражденията на персонала, допълнителни възнаграждения, данъчни и други задължения, трудов стаж и други подобни.

(2). Достъп до операционната система, съдържаща файловете за обработка на лични данни, имат само обработващите лични данни чрез персонална парола за отваряне на тези файлове, известна само на съответния служител, а в негово отсъствие, служителя който го замества със заповед на Директора на ЦСМП -Благоевград.

Чл.41(1). Компютърните конфигурации се поставят в общи помещения за работа на обработващия лични данни с изпълняващи други дейности, поради невъзможност за самостоятелно работно помещение.

РАЗДЕЛ IV. ПРАВА НА СУБЕКТИ НА ЛИЧНИ ДАННИ В ЦСМП - БЛАГОЕВГРАД

Чл.42. Според Регламента субектът на данни /физическото лице, за което се отнасят данните/ има право на:

1. Информираност;

Администраторът предоставя на субектите най-малко следната информация:

- Данните, които идентифицират администратора и координатите за връзка с него.
- Координатите за връзка с длъжностното лице по защита на данните, когато е приложимо.
- Категориите лични данни, които ще се обработват;
- Целите на обработването, за които са предназначени личните данни;
- Получателите или категориите получатели на лични данни;
- Правото да бъде подадена жалба до Комисията за защита на лични данни, координати за връзка;
- Дали личните данни ще бъдат предоставени в трета държава извън /ЕС, ЕИП/
- Целите и правното основание за обработването на личните данни, както и евентуалните последиствия, ако тези данни не бъдат предоставени;

- Срокове на съхранение на личните данни;
 - 2. Достъп до собствените си лични данни;
 - 3. Коригиране /ако данните са неточни/;
- Субектът на данни има право да поиска непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнително заявление.
- 4. Изтриване на личните данни /правото „да бъдеш забравен“/;
 - 5. Ограничаване на обработването от страна на администратора или обработващия лични данни;
 - 6. Преносимост на личните данни между отделните администратори;
 - 7. Възражение спрямо обработването на неговите лични данни;
 - 8. Субектът на данни има право и да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за субекта на данните или по подобен начин го засяга в значителна степен;
 - 9. Право на защита по съдебен или административен ред, в случай че правата на субекта на данни са били нарушени.

РАЗДЕЛ V. ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРИТЕ И ОБРАБОТВАЩИТЕ ЛИЧНИ ДАННИ

Чл.43. Задълженията на администраторите и обработващите лични данни са:

- 1. Обработване на данните в съответствие с принципите за защита на личните данни, заложен в Регламента, като е в състояние да докаже това /отчетност/.
- 2. Осигуряване на защита на данните на етапа на проектирането и по подразбиране;
- 3. Определяне на длъжностно лице по защита на личните данни в изрично посочените от регламента случаи./ако е приложимо/
- 4. Уведомяване на надзорния орган и субекта на данни в случай на нарушаване на сигурността на личните данни, както и документиране на всяко нарушение на сигурността на личните данни, в т.ч.фактите, свързани с нарушението, последиците от него, предприетите действия за справяне с нарушението.
- 5. Извършване на оценка на въздействието върху защита на данните.
- 6. Провеждане на предварителна консултация с надзорния орган преди обработването, когато оценката на въздействието покаже, че обработването ще породи висок риск, ако АЛД не предприеме мерки за ограничаване на риска.
- 7. Прилагане на подходящи технически и организационни мерки за осигуряване на сигурност на данните. /псевдонимизация, криптиране/
- 8. Гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите за обработване.
- 9. Своевременно възстановяване на наличността и достъпа на личните данни в случай на физически или технически инцидент.
- 10. Редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки.
- 11. Сътрудничество с надзорния орган за защита на личните данни при изпълнение на задълженията, произтичащи от регламента.

Чл.44.Администраторът предоставя лични данни в изпълнение на нормативно установени задължения.

Чл.45(1). Достъп до лични данни и разкриването им се осъществява по реда и при условията на ЗЗЛД от страна на следните лица:

- 1.Физически лица, за които се отнасят
- 2.Изрично упълномощени с нотариално заверено пълномощно представители на лицата по т.1.
- 3.Трето лице в случай, че е предвидено в нормативен акт.
- 4.Обработващият лични данни

(2).Достъпът се предоставя под форма на:

- устна или писмена справка

-преглед на данните

-предоставяне на копие от обработените данни

(3).При поискване АЛД предоставя копие от обработените лични данни на предпочитан носител или предоставяне по електронен път, освен в случаите, когато това е забранено от закон.

Чл.46(1).Правото на достъп и правата по чл.45 се осъществява писмено заявление /Приложение № 4/ до Директора на ЦСМП – Благоевград./може да се отправи и по електронен път/.

Съдържание на заявлението:

1.Име, адрес и други данни за идентифициране на съответното физическо лице

2.Описание на искането

3.Предпочитана форма за предоставяне на информация

4.Подпис,дата на подаване на заявлението и адрес за кореспонденция.

(2).При подаване на заявление от упълномощено лице към заявлението се прилага и нотариално заверено пълномощно.

(3).Заявленията се завеждат от технически сътрудник в АСС.

Чл.47(1).Администраторът разглежда заявлението по чл.46(1) и се произнася в 14-дневен срок от постъпването му в ЦСМП- Благоевград

(2).При заявленията за достъп АЛД разрешава пълен или частичен достъп на заявителя или мотивирано отказва извършването му.

(3).Срокът по ал.1 може да бъде удължен от администратора до 30 дни в определените ЗЗЛД случаи.

(4).Администраторът уведомява заявителя за решението си или отказа по ал.2 в съответно определения срок,лично срещу подпис или по пощата с обратна разписка.

(5).Липсата на уведомление по ал.4 се счита за отказ.

(6).Администраторът на лични данни е длъжен да се съобрази с предпочитаната от заявителя форма на предоставяне на информацията.

РАЗДЕЛ VII. РЕД ЗА УВЕДОМЯВАНЕ НА КЗЛД В СЛУЧАЙ НА НАРУШЕНИЕ СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ В ЦСМП-БЛАГОЕВГРАД

Чл. 48. (1) В случай на нарушение на сигурността на личните данни администраторът без излишно забавяне, но не по-късно от 72 часа след като е разбрал за него уведомява КЗЛД, освен ако няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица, когато уведомлението до КЗЛД не е подадено в срок до 72 часа, то се придружава от причините за забавянето.

(2) Обработващият лични данни на регистър „Персонал, регистър „Пациенти” и регистър „Видеонаблюдение” уведомява първо зав. ФСМП на съответния филиал в който е констатирано нарушението и лицето отговарящо за личните данни /Служител човешки ресурси/ в ЦСМП- Благоевград без излишно забавяне, след като е установил нарушение на сигурността на лични данни. Зав. ФСМП и Служител човешки ресурси уведомяват веднага директора на ЦСМП- Благоевград за констатираното нарушение.

(3) В уведомлението до КЗЛД, посочено в ал 1, се съдържа най-малко следното:

1.описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;

2.Посочване на 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;

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.

(4) Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

(5) Служител човешки ресурси документира всяко нарушение на сигурността на личните данни, посочено в ал. 1, в „Регистър на нарушения сигурността на личните данни в ЦСМП-Благоевград“ като включва фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на комисията да провери дали е спазен настоящият член.

Чл. 49. (1) Когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическите лица, администраторът без излишно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни.

(2) В съобщението до субекта на данните, посочено в ал. 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се съдържат най-малко информацията и мерките, посочени в чл. 48, ал. 3, точки 2, 3 и 4.

(3) Посоченото в ал. 1 съобщение до субекта на данните не се изисква, ако е изпълнено някое от следните условия:

1. администраторът е предприел 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 мерки, които правят личните данни неразбираеми за всяко лице, което няма право на достъп до тях, като например криптиране;

2. администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни, посочен в ал. 1;

3. то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

(4) Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, комисията може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да направи съобщението или да реши, че е изпълнено някое от условията по ал. 3.

(5) Съобщението до субекта на данните, посочено в ал. 1 от настоящия член, може да бъде забавено, ограничено или пропуснато, при условията и на основанията, посочени в чл. 54, ал. 3. От ЗЗЛД.

РАЗДЕЛ VIII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

&1. Настоящите правила са изготвени на основание Регламен 2016/679, влизащ в сила от 25.05.2018 г.

&2. Настоящите правила влизат в сила от деня на утвърждаването им със Заповед на Директора на ЦСМП- Благоевград.

&3. Изменение и допълнение на Правилата се извършва при промяна на нормативната уредба, указания от Мипистерство на здравоспазването, Комисия по защита на личните данни и въвеждане на нови регистри в ЦСМП- Благоевград, съдържащи лични данни на физически и юридически лица.

&4. Неразделна част към правилата са: Декларация за конфиденциалност /Приложение № 1/, Декларация за съгласие на служителите и работниците на ЦСМП – Благоевград за обработка на личните им данни /Приложение № 2/, Декларация за информирано съгласие на пациентите на ЦСМП – Благоевград за обработка на личните им данни/Приложение № 3/, Паспортизация на наличната техника /Приложение № 5/.

&5. За неспазване Правилата се прилагат санкциите от Регламен 2016/679.

Изготвил :

М.Танчева - Председател на комисия,
назначена със Заповед № 66/04.04.2018 г.
на Директора на ЦСМП-Благоевград

ДЕКЛАРАЦИЯ

Подписаният/та.....

(име, презиме и фамилия)

на длъжност.....В.....

(структурно звено)

На основание Правила за начина на обработване на лични данни и водене на регистри по закона за защита на личните данни в ЦСМП- Благоевград, Етичен кодекс, ПУДВР и др.

ДЕКЛАРИРАМ, ЧЕ :

1. Ще пазя в тайна личните данни на трети лица, станали ми известни при изпълнение на служебните ми задължения, няма да ги разпространявам и няма да ги използвам за други цели освен за прякото изпълнение на служебните ми задължения.
2. Запознат/а/ съм с нормативната уредба, политиката и ръководствата в областта на защита на личните данни, както и със съдържанието на Правила за начина на обработване на лични данни и водене на регистри по закона за защита на личните данни в ЦСМП- Благоевград
3. Запознат/а/ съм, че при разгласяване, предоставяне, публикуване, използване или разпространяване по друг начин на факти и обстоятелства, представляващи лични данни носят дисциплинарна отговорност по Кодекса на труда, административно-наказателна отговорност по Закона за защита на личните данни и наказателна отговорност, ако деянието осъществява състава на чл. 284 и /или на чл. 319д от Наказателния кодекс.

Дата:.....

ДЕКЛАРАТОР:.....

(подпис)

ДЕКЛАРАЦИЯ

Долуподписаният/ата

С адрес:.....

ДЕКЛАРИРАМ:

Съгласен/а съм ЦСМП- Благоевград да обработва и съхранява личните ми данни, съгласно изискванията на Регламент /ЕС/ 2016/679 на Европейския парламент и на Съвета, Закона за защита на лични данни, които предоставям във връзка с подаване на заявление/молба за назначаване на работа.

Запознат/а съм с:

- целта и средствата на обработка на личните ми данни;
- доброволния характер на предоставянето на данните;
- правото на достъп и на коригиране на събраните данни.

С настоящата декларация декларирам съгласие за съхранение и обработка на личните ми данни при спазване на разпоредбите на Закона за защита на личните данни.

Дата.....

Гр.

ДЕКЛАРАТОР:.....

ЦЕНТЪР ЗА СПЕШНА МЕДИЦИНСКА ПОМОЩ – БЛАГОЕВГРАД

ДЕКЛАРАЦИЯ

ЗА ИНФОРМИРАНО СЪГЛАСИЕ НА ПАЦИЕНТА

Уважаеми господине / госпожо,

Вие имате право като пациент на ЦСМП- Благоевград да бъдете информиран за състоянието си, така че да можете да дадете или откажете съгласието си за предстоящото оказване на спешна медицинска помощ. Ваше право е както да се съгласите, така и да откажете оказването на спешна медицинска помощ.

Долуподписаният/ната

С адрес:.....

//име, презиме, фамилия на пациента/

Родител, настойник, попечител/на

I. Декларирам, че бях подробно запознат относно:

1. Диагнозата и характера на заболяването.
2. Целите на оказване на спешна медицинска помощ, очакваните резултати и прогнозата.
3. Потенциалните рискове, свързани със странични ефекти, болка и други неудобства.

II. Съгласен/а съм ЦСМП- Благоевград да обработва и съхранява личните ми данни, съгласно изискванията на Регламент /ЕС/ 2016/679 на Европейския парламент и на Съвета, Закона за защита на лични данни, които предоставям във връзка с оказване на спешна медицинска помощ.

Запознат/а съм с:

- целта и средствата на обработка на личните ми данни;
- доброволния характер на предоставянето на данните;
- правото на достъп и на коригиране на събраните данни.

С настоящата декларация декларирам съгласие за съхранение и обработка на личните ми данни при спазване на разпоредбите на Регламент /ЕС/ 2016/679 на Европейския парламент и на Съвета и Закона за защита на личните данни.

ЗАЯВАВАМ, ЧЕ НАСТОЯЩИЯТ ФОРМУЛЯР МИ БЕ РАЗЯСНЕН НА РАЗБИРАЕМ И ДОСТЪПЕН ЕЗИК

.....
/дата/

Декларатор.....
/подпис/

ДО
ДИРЕКТОРА
НА ЦСМП
ГР. БЛАГОЕВГРАД

З А Я В Л Е Н И Е

За достъп до лични данни съгласно ЗЗЛД

От.....
/трите имена/

.....
/точен адрес/

ОТНОСНО:.....
.....
/описание на исканото/

Исканата информация да бъде предоставена под формата
на.....
/устна , писмена справка, преглед на данните/

При подаване на заявление от упълномощено лице освен данните по ал. 1 се прилагат и данните на опълномощения в съответно пълномощно №.....

Дата:.....
Гр.....

Подпис:

Адрес за кореспонденция:

.....
Длъжностно лице приело заявлението:

Паспортизация

Сервър								
№	Процесор	Памет	Диск	Операционна Система	Офис пакет	Антивирусна програма	Информационни системи / Програми	
1	Intel Core i3-4150	6.0 GB	1000GB	windows 10 home, 64 bit		avast	Терес, Скипър	Сервър
Входни точки - работни станции								
№	Процесор	Памет	Диск	Операционна Система	Офис пакет	Антивирусна програма	Информационни системи / Програми	Длъжности, обработващи лични
1	Intel Core i3-4150	6.0 GB	1000GB	windows 8 home, 64 bit	microsoft office 2007	avast	ЕП, Терес, 112	икон. ТРЗ
2	Intel Pentium J2900	4.0 GB	500GB	windows 10 home, 64 bit	microsoft office 2007	avira	ЕП, Терес, 112	служ. Човешки ресурси
3	Intel Pentium G3260	4.0 GB	160GB	windows 7 pro, 64 bit	microsoft office 2007	avast	Скипър	счетоводител
4	Intel Core Duo E4500	2.0 GB	250GB	windows 7 pro, 32 bit	microsoft office 2007	avira	ЕП, Терес, 112	каснер
5	Intel Pentium 4, 3.0GHz	1.0 GB	500GB	windows XP, 32 bit	microsoft office 2007	avast	112	гл.мед.сестра
6	Intel Pentium J2900	4.0 GB	500GB	windows 10 home, 64 bit	microsoft office 2007	avast	Скипър, 112	техн.сътрудник

Легенда: ЕП - електронен подпис
Терес е програмни продукт - ТРЗ и ЛС
Скипър - счетоводна програма

Мрежово оборудване - рутер, свич

№	Производител	Модел	Безжичен	WiFi	Защита	Други	Брой
1	D-Link	DIR-301 Wireless G Router	Да	54Mbit/s, 802.11b, 802.11g	WPA, VPN, Firewall	портове: 4 x 10/100 Base-T	1
2	D-Link	DGS-1008D	Не	Не	Не	портове: 8 x 10/100/1000 Base-T	2

Външни носители - USB диск, USB флашки, CD, DVD дискове

№	Производител	Модел
1	Seagate	USB, 3.5", 1.0GB

Изготвил:
инж. Георги Лазаров
IT специалист