УТВЪРДИЛ:...../п/.....

Д-Р ГЕНАДИ СТРАНДЖЕВ

/УПРАВИТЕЛ/

ИНСТРУКЦИЯ ЗА МЕРКИТЕ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, СЪБИРАНИ, ОБРАБОТВАНИ, СЪХРАНЯВАНИ И ПРЕДОСТАВЯНИ ОТ МБАЛ „СВЕТИ МИНА”- ПЛОВДИВ ЕООД

РАЗДЕЛ ПЪРВИ
ОБЩИ ПОЛОЖЕНИЯ

Чл. 1. Настоящата инструкция урежда организацията и вътрешния ред на МБАЛ„Свети Мина”- Пловдив ЕООД, като администратор на лични данни, както и нивото на технически и организационни мерки при обработване на лични данни и допустимия вид защита.

Чл.2. Инструкцията е изготвена в съответствие с изискванията на Общия регламент за защита на данни Регламент (ЕС)2016/679 (ОРЗД), Закона за защита на личните данни (ЗЗЛД) и цели защита интересите на клиентите – физически и юридически лица, както и на служителите на МБАЛ „Свети Мина”- Пловдив ЕООД (за краткост, наричано по-долу МБАЛ)от незаконосъобразно и недобросъвестно обработване на личните им данни.

Чл.3.(1) Настоящата инструкция регламентира:

1. Механизмите за водене, поддържане и защита на регистрите, съхраняващи лични данни в МБАЛ с цел гарантиране на неприкосновеността на личността и личния живот, чрез осигуряване на защита на данните за физическите лица при неправомерно обработване на свързаните с тях лични данни в процеса на свободното движение на данните.
2. Видовете регистри, които се водят в МБАЛ и тяхното общо и технологично описание.
3. Правата и задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения.
4. Необходимите технически и организационни мерки за защита на личните данни, съдържащи се в регистрите от неправомерно обработване (случайно или незаконно разрушаване, случайна загуба или промяна, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни).
5. Процедури за докладване, управляване и реагиране при инциденти. Организацията и реда за упражняване на контрол при обработването на лични данни от служителите на МБАЛ.
6. Оценка на въздействие и определяне ниво на защита.

7. Предоставяне на данни на трети лица – основание, цел, категории лични данни.
(2) Инструкцията се утвърждава, допълва, изменя или отменя със заповед на Управителя на МБАЛ.
Чл.4.(1) МБАЛ обработва само законно събрани лични данни, необходими за конкретни, точно определени и законни цели. Личните данни, които МБАЛ събира и обработва следва да бъдат точни и при необходимост да се актуализират. Личните данни се заличават или коригират, когато се установи, че са неточни или несъответстващи на целите, за които се обработват.
(2) МБАЛ поддържа личните данни във вида и формата, които позволяват идентифициране самоличността на физическите лица за срок не по-дълъг от необходимия за изпълнение на целите, за които личните данни се обработват.
(3) МБАЛ спазва принципа за забрана на обработване на специални категории данни съгласно чл. 5, ал. 1 от ЗЗЛД (разкриване на расов или етнически произход; разкриване на политически, религиозни или философски убеждения; членство в политически партии или организации; сдружения с религиозни, философски, политически или синдикални цели; лични данни, които се отнасят до здравето, сексуалния живот или до човешкия геном), като изключения се допускат само в случаите, предвидени в чл. 5, ал. 2 от ЗЗЛД, в чиято хипотеза попада МБАЛ.
Чл.5.(1) Субектът - притежател на личните данни - изразява свободно своето съгласие относно обработването на отнасящи се за него лични данни.
(2) Субектът има право по всяко време на обработването да поиска блокиране или унищожаване (изтриване) на събрани за него лични данни, в случаите, когато оспорва тяхната точност или обработването им е незаконосъобразно.
(3) В случаите, когато данните не са получени от субекта, МБАЛ го информира за целите и правното основание на обработването, за категориите предоставени данни и техния източник, за получателите, на които ще бъдат предоставени, както и за правото му на достъп до неговите лични данни.
Чл.6. Като администратор на лични данни по смисъла на чл.3, ал.1 от ЗЗЛД, МБАЛ поддържа личните данни във вид, който позволява идентифициране на физическите лица.

РАЗДЕЛ ВТОРИ
ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ

Чл. 7. (1) Обработване на личните данни се извършва, когато:
1. това е необходимо за изпълнение на нормативно установено задължение;
2. физическото лице, за което се отнасят данните, е дало своето изрично съгласие. Субектите (физически лица и представляващите юридически лица) и служителите на МБАЛ, се идентифицират посредством официален документ за самоличност (лична карта). Документът за самоличност при необходимост се копира като субектът изписва на копието „Съгласен/а съм с копирането" и се подписва върху него. Оригиналът се връща на субекта, а копието се съхранява за срок от 5 години.
3. обработването е необходимо за изпълнение на задължения по договор, по който физическото лице, за което се отнасят данните, е страна, както и за действия, предхождащи сключването на договор и предприети по негово искане.
4. обработването е необходимо, за да се защитят животът и здравето на физическото лице, за което се отнасят данните;
5. обработването е необходимо за изпълнението на задача, която се осъществява в обществен интерес;

6. обработването е необходимо за упражняване на правомощия, предоставени със закон на администратора или на трето лице, на което се разкриват данните;
7.обработването е необходимо за реализиране на законните интереси на администратора на лични данни или на трето лице, на което се разкриват данните, освен когато пред тези интереси преимущество имат интересите на физическото лице, за което се отнасят данните.
(2) Обработване на личните данни се състои и в осигуряване на достъпа до определена информация само за лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп.
Чл.8. (1) Всички служители на МБАЛ при встъпване в длъжност приемат да спазват конфиденциалност по отношение на базите данни с клиенти на МБАЛ „Свети Мина"-Пловдив ЕООД, в т. ч. лични данни, както и да не разгласяват данни и информация, станали им известни при и по повод изпълнение на служебните им задължения.
(2) Достъпът до лични данни се осъществява само от лица, чиито служебни задължения или конкретно възложена задача налагат такъв достъп, при спазване на принципа „Необходимост да знае" и след запознаване с нормативната уредба в областта на защитата на личните данни, политиката и ръководствата за защита на личните данни и опасностите за личните данни, обработвани от администратора, като за целта лицата подписват декларация за неразгласяване на лични данни на основание чл.7, ал.5 от Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните дани, до които са получили достъп при и по повод изпълнение на задълженията си.
(3) Всички лица, отговарят за спазването на ограниченията за достъп до личните данни, и са персонално отговорни пред Управителя на МБАЛ за нарушаването на принципите за поверителност, цялостност и наличност на личните данни, освен в случаите на форсмажорни обстоятелства.
Чл.9. МБАЛ поддържа вътрешен ред като администратор на лични данни, като осигурява технически и организационни мерки за защита.
Чл. 10. (1) Администраторът възлага обработването на личните данни на негови служители /обработващи/. Обработването се възлага на повече от един обработващ данните, съобразно спецификата на изпълняваните от тях служебни функции и с цел разграничаване на конкретните им задължения.
(2) Обработващите лични данни, действат само по указание на администратора, освен ако в закон не е предвидено друго.
Чл. 11. (1) Личните данни в регистрите се набират от администратора на лични данни, респективно обработващият лични данни чрез устно интервю и/или на хартиен и/или електронен носител (за служители), чрез предоставени епикризи, лабораторни изследвания, ретгенови и ехографски снимки, както и такива, изведени в хода на лечението на заболяването (за пациенти); за контрагенти на МБАЛ - чрез електронни фактури и/или на хартиен носител, както и носители с лични данни, необходими за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор.
(2) За необходимостта от набиране на лични данни и целите, за които ще бъдат използвани, обработващият лични данни информира лицето.
(3) След одобрение на документите, съдържащи лични данни от ресорния ръководител, същите заедно с приложенията към тях се обработват в регистрите от обработващия лични данни и се съхраняват в дискови масиви. Резервни копия се създават на дискови масиви, магнитни или магнитооптични носители, като тези копия се съхраняват в помещения с контролиран достъп. При необходимост, в случаи, свързани с опазване на

обществения ред се създават извадки от видеозаписи на магнитен или магнитооптичен носител.

Достъп до операционната система, съдържаща файлове за обработка на лични данни, имат само обработващите на лични данни чрез парола за отваряне на тези файлове. Защитата на електронните данни от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на антивирусни програми, периодично архивиране на данните на отделни дискети, както и чрез поддържане на информацията на хартиен носител.

(4) Набраните данни на технически носител остават на сървъри, предназначени за съхранение на базите с лични данни, а в случаите, когато се обработват на компютри извън мрежата на администратора - в отделни файлове на компютъра, като достъп до тях има само обработващият лични данни чрез съответните потребителски имена и пароли.
(5) Хартиеният носител се подрежда в кадрови досиета/пациентски досиета или специални папки и се представя за проверка законосъобразността на изготвения документ и валидирането му чрез подписи на съответните длъжностни лица - Управител, Заместник Управител, Главна сестра, Началник отделение, Лекуващ лекар, Приемащ лекар и т.н..
(6) При необходимост от поправка на личните данни, лицата предоставят такива на обработващия лични данни по негово искане на основание нормативно задължение.
(7) За достоверността на предоставените копия от регистри, съдържащи лични данни, отговорност носи обработващият лични данни.

РАЗДЕЛ ТРЕТИ
ОБЩО ОПИСАНИЕ НА ПОДДЪРЖАНИТЕ РЕГИСТРИ В МБАЛ ”СВЕТИ МИНА ПЛОВДИВ” ЕООД

Чл. 12. (1) Регистрите в които се набират и съхраняват лични данни са за:
1. физически лица в Република България, посетили лечебното заведение по повод здравословното си състояние.
2. служителите по трудово и служебно правоотношение в лечебното заведение;
3. контрагенти, с които МБАЛ има договорни отношения.
(2) Категориите лични данни в регистрите, които се отнасят се до физическите лица могат да бъдат:
Физическа идентичност - име, ЕГН/ЛНЧ, номер на лична карта, дата и място на издаване, адрес, месторождение, телефони за връзка, един или повече специфични признаци и други;
Семейната идентичност - семейно положение (наличие на брак, развод, брой членове на семейството, в т.ч. деца до 18 години), родствени връзки и др.;
Образование - вид на образованието, място, номер и дата на издаване на дипломата, допълнителна квалификация. Предоставят се от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
Допълнителна квалификация – данните се предоставят от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
Трудова дейност - професионална биография - данните се предоставят от лицата на основание нормативно задължение във всички случаи, когато е необходимо;
Медицински данни – физиологично, психическо и психологично състояние на лицата. Данните са от значение при заемане на длъжности и изпълнение на функции,

изискващи особено висока степен на отговорност, пряка ангажираност и непосредствен досег с хора, в това число от рискови групи; „*Данни за здравословното състояние*“ - лични данни, свързани с физическото или психическото здраве на физическо лице-чувствителни лични данни;
Икономическа идентичност - имотно състояние, финансово състояние, участие и/или притежаване на дялове или ценни книжа в дружества и др.;
Други - лични данни относно гражданско-правния статус на лицата, необходими за длъжностите, свързани с материална отговорност. Предоставят се на основание нормативно задължение.
(3) Видовете регистри, поддържани в МБАЛ; категориите лични данни в тях; технологичното описание - носители на данни, технология на обработване, срок на съхранение, нива на защита и мерки са описани в **Приложение № 1**, представляващонеразделна част от настоящата Инструкция.

РАЗДЕЛ ЧЕТВЪРТИ
ДЛЪЖНОСТИ, СВЪРЗАНИ С ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ. ПРАВА И ЗАДЪЛЖЕНИЯ

Чл. 13.(1) Служителите от МБАЛ са длъжни да спазват и изпълняват тази инструкция, в съответствие с длъжностните им характеристики.
Чл.14.(1) Със Заповед или друг нормативен акт Управителят определя лицата по защита на информацията.
(2) Лицето по защита на информация има следните правомощия:
1. консултативни функции в областта на защитата на личните данни, надзор по спазването на регламента в организацията на администратора;
2. да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на нормативните актове за защита на личните данни;
3. да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни 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;
4. поддържа връзка с Комисията за защита на личните данни относно подадените заявления за предоставяне на лични данни;
5. да си сътрудничи с надзорния орган.
(3) Системният администратор има следните правомощия:
1. осигурява организацията по водене на регистрите, съгласно предвидените мерки за гарантиране на адекватна защита;
2. следи за спазването на конкретните мерки за защита и контрол на достъпа съобразно, спецификата на водените регистри;
3. осъществява контрол по спазване на изискванията за защита на регистрите;
4. поддържа връзка с Комисията за защита на личните данни относно предприетите мерки и средства за защита на регистрите;
5. контролира спазването на правата на потребителите във връзка с регистрите и програмно техническите ресурси за тяхната обработка;
6. специфицира техническите ресурси, прилагани за обработка на личните данни;

7. следи за спазване на организационната процедура за обработване на личните данни, включваща време, място и ред при обработване, като чрез регистрация на всички извършени действия с регистрите в компютърната среда.
8. определя ред за съхраняване и унищожаване на информационни носители, заедно с юрисконсулт;
9. определя ред при задаване, използване и промяна на пароли, както и действията в случай на узнаване на парола и/или криптографски ключ;
10. определя правила за провеждане на редовна профилактика на компютърните и комуникационните средства, включваща и проверка за вируси, за нелегално инсталиран софтуер, на целостта на базата данни, както и архивиране на данни, актуализиране на системната информация и др.;
11. провежда периодичен контрол за спазване на изискванията по защита на данните и при открити нередности взема мерки за тяхното отстраняване.
Чл.15.(1) Със Заповед или друг нормативен акт Управителят определя обработващите лични данни за различните видове регистри.
(2) Обработващите лични данни се задължават:
1. да обработват лични данни законосъобразно и добросъвестно;
2. 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;
3. да актуализират регистрите на личните данни (при необходимост);
4. да заличават или коригират личните данни, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
5. 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;
6. да не допускат неоторизирани лица в помещенията, в които се съхраняват данните.
Чл. 16. (1) За обработване на регистри, съдържащи лични данни служителят подписва декларация, че е запознат със Закона за защита на личните данни и с настоящата Инструкция за защитата на личните данни, които се обработват от него.
(2) Декларацията по ал. 1 се предоставя от служител в дирекция „Човешки ресурси“ и след попълване от страна на лицето се съхранява в личното му досие.
(3) За неизпълнение на задълженията вменени на съответните длъжностни лица по тази Инструкция и по Закона за защита на личните данни, се налагат дисциплинарни наказания по Кодекса на труда и други специализирани закони, а когато неизпълнението на съответното задължение е констатирано и установено от компетентен орган, предвиденото в Закона за защита на личните данни административно наказание - глоба. Ако в резултат действията на съответното длъжностно лице по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред, ако стореното представлява по-тежко деяние, за което се предвижда наказателна отговорност.
Чл. 17. (1) Администраторът предоставя лични данни в изпълнение на нормативно установени задължения и в случаи, свързани с опазване на обществения ред.
(2) Лични данни се предоставят служебно между отделенията/отделите в МБАЛ след обосновано искане.
(3) Достъп до лични данни на лицата, съдържащи се на технически носител имат само определеният със заповед на Управителя на МБАЛ обработващ лични данни, който чрез парола има достъп до информацията и до съответния компютър.
(4) Освен на обработващият лични данни, правомерен е и достъпът на длъжностните лица, пряко ангажирани с оформянето и проверка законосъобразността на документите

на лицата – Заместник Управител, Гл. Счетоводител, Гл. Сестра, Началник отдели/отделения, отговарящи за съответния ресор, в който се водят регистри. Обработващият лични данни е длъжен да им осигури достъп при поискване от тяхна страна.

РАЗДЕЛ ПЕТИ
ОЦЕНКА НА ВЪЗДЕЙСТВИЕ

Чл. 18.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, цялостността или наличността на личните данни.
Чл. 19.Нивата на защита на поддържаните от МБАЛ регистри са посочени в **Приложение № 1**.

РАЗДЕЛ ШЕСТИ
ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ

МБАЛ предприема следните мерки за защита на личните данни – технически и организационни:
(1) програмно-технически – надеждна и защитена идентификация и автентификация на лицата, които обработват лични данни в електронен вид чрез пароли за достъп и определени потребителски права за работа с данните; поддържане на електронен архив и редовно архивиране на информационните бази, съдържащи лични данни; поддържане на операционните системи в актуално състояние; поддържане на антивирусни програми в актуално състояние; ползване на електронен подпис.
(3) физически – система от мерки по защита на сградите, помещенията и съоръженията, в които се създават, обработват и съхраняват лични данни и контрола върху достъпа до тях: личните данни се съхраняват в специализирани помещения или в зони с ограничен достъп.
(4) организационни и административни – регламентирани с правила и заповеди на Управителя на МБАЛ;
(5) нормативни, предвидени в законови и подзаконови нормативни актове.

РАЗДЕЛ СЕДМИ
ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ

Чл. 20. МБАЛ предприема превантивни действия при защита на личните данни в случай на настъпили природни бедствия. Изпълняват се основните задължения по плана на МБАЛ за защита при бедствия със специализираните си части за действия при наводнения, пожари, земетресения, свлачищни процеси, терористичен акт или други инциденти, застрашаващи живота и здравето на хората. При настъпили критични ситуации, правилото е спасяване на човешки животи и последващи действия за опазване и защита на личните данни.
1. Конкретни действия при настъпили бедствени ситуации:
- защита от пожари –при задействане на пожароизвестителната система и установяване на пожар, се започва незабавно гасене със собствени средства /пожарогасители/и уведомяване на съответните органи; Евакуация на служители и посетители от сградата.

Като превантивна мярка за опазване на личните данни, същите е необходимо да се съхраняват в специално предназначени шкафове.
- защита от наводнения - предприемат се незабавни действия по ограничаване на разпространението, както и се изпомпва водата или загребва със собствени подръчни средства; евакуират се служители и посетители. Като превантивна мярка за опазване на личните данни, същите е необходимо да се съхраняват в специално предназначени шкафове.
- при други възможни критични ситуации, служителите работещите с лични данни е необходимо да прилагат по-горе цитираната превантивна мярка.

РАЗДЕЛ ОСМИ
ПРЕДОСТАВЯНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ЛИЦА

Чл. 21.(1) Лични данни се предоставят на трети лица само след получаване на писмено съгласие от лицето, за което се отнасят данните, освен в случаите, когато това е предвидено с нормативен акт, както и случаи, свързани с опазване на обществения ред и сигурността.
(2) При неполучаване на съгласие от лицето или при изричен отказ да се даде съгласие, данните не се предоставят.
(3) Не се изисква съгласие на лицето, ако обработването на неговите лични данни се извършва само от или под контрола на компетентен държавен орган за лични данни, свързани с извършване на престъпления, на административни нарушения и на непозволени увреждания.
(4) Решението си за предоставяне или отказване достъп до лични данни за съответното лице администраторът съобщава на третото лице в 30 - дневен срок от подаване на искането.
Чл. 22.(1) Регистрите, съдържащи лични данни не се изнасят извън сградата на администратора. Никое длъжностно лице или трето лице няма право на достъп до регистрите с лични данни, освен ако данни от същите не са изискани по надлежен път от органи на съдебната власт (съд, прокуратура, следствени органи). В такива случаи достъпът е правомерен.
(2) Правомерен е и достъпът на ревизиращите държавни органи, надлежно легитимирали се 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 им се осигури достъп до лични данни.
(3) Съдебен орган може да изиска лични данни, съдържащи се в регистри, писмено с изрично искане, отправено до Управителя на МБАЛ. В подобни случаи, на органите на съдебната власт, се предоставя копие от съдържащите се в регистрите лични данни, заверени с подписа на обработващия лични данни и печат на МБАЛ. За идентичността на предоставените копия от документи с оригиналите им, отговорност носи обработващият лични данни. В подобни случаи и ако в писменото искане на съдебния орган не се съдържа изрична забрана за разгласяване, обработващият лични данни е длъжен да информира лицето, но не и да възпрепятства работата на съответните органи.
(4) Обработването на лични данни за целите на превенцията на изпирането на пари и финансирането на тероризма се смята за въпрос от обществен интерес съгласно GDPR и не може да бъде ограничено от изискванията на чл. 12 – 22 и чл.34 от същия регламент.

(5) ЗМИП изисква събирането, обработването и използването на лични данни за изпълнение на няколко основни задачи в процеса на противодействие на използването на финансовата система за целите на изпирането на пари, които могат да бъдат обобщени по следния начин:

- комплексна проверка на клиента *(включително разширена и опростена проверка)*;
- мониторинг на транзакции и на поведение;
- вътрешно споделяне на данни *(включително в рамките на група)*;
- споделяне на данни извън организацията *(включително с външни изпълнители, регулаторни органи и други финансови институции)*;
- трансгранично обработване на данни *(особено при обработването на международни плащания)*.

(6) Ообработването на лични данни от задължените субекти по чл.4 от ЗМИП трябва да е съобразено, на първо място, с принципите, установени в чл.5 от GDPR, и наред с това с всички останали негови разпоредби.

(7) Според чл.5 от GDPR личните данни следва да са:

- обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните *(„законосъобразност, добросъвестност и прозрачност“)*;
- събирани за конкретни, изрично указани и легитимни цели и да 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, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели *(„ограничение на целите“)*;
- подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват *(„свеждане на данните до минимум“)*;
- точни и при необходимост да бъдат поддържани в актуален вид, като се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват *(„точност“)*;
- 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 съгласно член 89, параграф 1, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в този регламент, с цел да бъдат гарантирани правата и свободите на субекта на данните *(„ограничение на съхранението“)*;
- 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 организационни мерки *(„цялостност и поверителност“)*.

Седмият принцип, свързан със защитата на личните данни, по чл. 5 от GDPR – принципът на отчетност, задължава администраторите на лични данни да документират и да са в състояние да доказват във всеки един момент спазването на останалите шест принципа и на изискванията на регламента.

РАЗДЕЛ ДЕВЕТИ
СЪХРАНЯВАНЕ И УНИЩОЖАВАНЕ НА ЛИЧНИ ДАННИ

Чл. 23. Лични данни на физическите и юридическите лица, получени за целите, за които се обработват, се съхраняват съгласно сроковете приети с нормативни актове за тяхното съхранение в МБАЛ, съответно за период не по-дълъг от необходимия, съгласно съответните цели, за които се използват.
Чл.24. След постигане целите по предходния член личните данни на физическите и юридическите лица се унищожават физически, чрез машинно нарязване или се предават за изгаряне, за което надеждно се изготвят актови протоколи за унищожаване.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. По смисъла на тези Инструкция:
„Лични данни“ са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци.
„Администратор на лични данни” е МБАЛ „Свети Мина”- Пловдив ЕООД, представлявана от Управителя на МБАЛ, която самостоятелно или чрез възлагане на друго лице обработва лични данни.
"Обработване на лични данни" е всяко действие или съвкупност от действия, които могат да се извършват по отношение на личните данни с автоматични или други средства, като събиране, записване, организиране, съхраняване, адаптиране или изменение, възстановяване, консултиране, употреба, разкриване чрез предаване, разпространяване, предоставяне, актуализиране или комбиниране, блокиране, заличаване или унищожаване.
„Обработващилични данни” са длъжностни лица от лечебното заведение, определени със Заповед от Управителя на МБАЛ или длъжностните характеристики, на които включват дейности, които изискват обработване на лични данни.
"Регистър на лични данни" е всяка структурирана съвкупност от лични данни, достъпна по определени критерии, централизирана, децентрализирана или разпределена на функционален или географски принцип.
„Лице по защита на информацията“ е физическо лице, притежаващо необходимата компетентност, което е упълномощено или назначено от администратора със съответен писмен акт, в който са уредени правата и задълженията му във връзка с осигуряване на необходимите технически и организационни мерки за защита на личните данни.
„Трето лице“ е физическо или юридическо лице, орган на държавната власт или местно самоуправление, различен от физическото лице, за което се отнасят данните, от администратора на лични данни, от обработващия лични данни и от лицата, които под прякото ръководство на администратора или обработващия имат право да обработват лични данни.
"Поверителност" е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

"Цялостност" е изискване данните да не могат да бъдат променени/подменени по неоторизиран начин в процеса на тяхното обработване и изискване да не се дава възможност за изменение и за неразрешени манипулации на функциите по обработване на данните.
"Наличност" е изискване за осигуряване непрекъсната възможност за обработване на личните данни на оторизираните лица и за изпълнение на функциите на системата за обработване или бързото им възстановяване.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Настоящата инструкция се издава на основание чл. 23, ал. 4 от Закона за защита на личните данни и чл. 19 т. 2 от Наредбата № 1 от 30.01.2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни.
§ 2. За допуснати нарушения по настоящата инструкция, виновните длъжностни лица носят дисциплинарна и административно-наказателна отговорност, освен ако деянието не представлява престъпление.
§ 3. За неуредените в тази инструкция въпроси се прилагат разпоредбите на действащата нормативна уредба.
§4. Контролът по прилагането и спазването на тази инструкция се осъществява от Управителя на МБАЛ „Свети Мина Пловдив" ЕООД.
§ 5. Настоящата инструкция влиза в сила от деня на нейното утвърждаване със заповед на Управителя на МБАЛ, както и Приложение 1 по чл.12,ал.3 от Инструкцията.
§ 6. Настоящите Вътрешни правила са изменени със Заповед №ОА-57/29.05.2019 г.
§ 7. В случай на нормативни изменения през време на действието на настоящите правила, в резултат на които някои техни норми частично или напълно се окажат в противоречие с новите разпоредби, последните се прилагат директно.

Приложение № 1

ВИДОВЕ РЕГИСТРИ, КОИТО СЕ ПОДЪРЖАТ В МБАЛ „СВЕТИ МИНА ПЛОВДИВ” ЕООД

Видове регистри/ отдел-отговорник	**категории лични данни**	**основание за обработване**	**носители на данни**	**технология на обработване**	**Срок на съхранение**	**Ниво на защита/ предприети мерки**
в Регистри „Персонал”в т.ч.: Регистър „Трудови договори” Регистър за изменение на трудовите договори Регистър за прекратяване на трудовите договори Регистър извънтрудови правоотношения Регистър за специализанти Регистър за издадени удост-я за трудов и осиг. стаж Регистър за събиране на данни от осигурителите за осигурените лица Регистър на издадените трудови книжки	ЕГН/ЛНЧ, гражданство, семейно положение, постоянен адрес и документ за самоличност, който се връща веднага, копия на документи, удостоверяващи образование и квалификация, трудова дейност, банкова сметка	КСО, КТ, ЗВО, закони и подзаконови актове на НОИ, НАП, ИТ, БЛС, ЗЗЛД – (чл.12, ал.1, т.1 вр. ал.2 и 4 от Закона за сч-вото; чл.52 и т.9, параграф 1 от ДР на Закона за националния архивен фонд; чл.39, т.3 от Наредба за реда, организирането, обработването, експертизата, съхраняването и използването на документите в учрежденските архиви на държавните и общинските институции;	Хартиен, електронен носител	При обработване на трудови досиета-всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и гражданските правоотношения –за изготвяне на всякакви документи на лицата в тази връзка (договори, допълнителни споразумения; документи, удостоверяващи трудов стаж; служебни бележки; справки; удостоверения и др. подобни)	Трудов договор (анекси към тр.д-р, др. документи от трудовото досие, пряко свързани с начисляването и изплащането на заплати) - 50 години; срок за съхранение на лични данни на участници в процедури по набиране и подбор на персонала – до 6 м.; автобиография, копия от дипломи за придобито образование, удостоверения/сертификати, препоръки, удостоверение за банкова см/ка – 3 г. след прекратяване на тр. Правоотношение;	Високо /В шкафове с ключалки.В работни помещения; Лична парола за достъп; Сървър; СОТ

Регистър на служебните досиета Ругистър за приети болнични листове Регистър за установяване и отчитане на трудови злополуки Отговорник:служител ЛС и ОНОТ		чл.5, ал.1 от КСО; чл.56 и чл.54, ал.4 от Наредба за медицинската експертиза			болнични листове – 3 г., считано от 1 януари на годината, следваща годината, в която са издадени; анулирани болнични листове – 3 г. след датата на издаването им	
Регистър „Пациенти” в т.ч.: Регистър преминали болни Регистър раждания Регистър новородени Регистър избор лекар/екип Диспансерен регистър Отговорник: Зам.упр.по мед.д-ст, Гл. Мед. сестра	ЕГН/ЛНЧ, гражданство, семейно положение, постоянен адрес, тел., имена, документ за самоличност, степен на образование	ЗЗО, ЗЛЗ, НАРЕДБА № 1 от 27.02.2013 г. за предоставяне на медико-статистическа информация и на информация за мед. дейност на ЛЗ; закони и подзаконови актове на МЗ, НЗОК, РЗОК, ИАМО, РЗИ, НЦОЗА, ЗЗЛД	Хартиен, електронен носител	Регистрация на Здравна информация – чл. 27 от ЗЗ - лични данни, свързани със здравословното състояние, физическото и психическото развитие на лицата и всяка друга информация в медицинската документация - чувствителни лични данни съгл. чл.5, ал. 1, т.3 от ЗЗЛД Създаване на Електронно досие на пациента - съдържа информация за извършени прегледи, консултации, образни, функционални и лабораторни изследвания, както и история на извършените хоспитализации на пациента в лечебното заведение. Регистрация на паспортни данни на пациент (български и чужди граждани) с различни източници на финансиране (НЗОК, ДЗЗФ и др.), печат на пациентска карта, проверка на здравноосигурителни		Изключително високо/В шкафове с ключалки.В работни помещения; Лична парола за достъп; Сървър; СОТ

				права, планиране на заетостта на ресурсите по кабинети, персонал или апаратура, заплащане на потребителски такси и други услуги по платения ценоразпис на лечебното заведение;		
Регистър „Счетоводство” в т.ч.: Регистър „Контрагенти” Регистър „Ведомости заплати” Регистър „Извънтрудови правоотношения” Отговорник: Гл. счетоводител	БУЛСТАТ, имена на МОЛ, наименование фирма-контрагент; имена и ЕГН-та, банкови с/ки на служители; Идентифициране на физически лица съгл. ЗМИП: датата и мястото на раждане; официален личен идентификационе н номер или друг уникален елемент за установяване на самоличността, съдържащ се в официален документ за самоличност, чийто срок на валидност не е изтекъл и на който има снимка на клиента; всяко гражданство, което лицето притежава; държава на постоянно пребиваване и	Закон за счетоводството, МСС, Търговски регистър, ЗДДС, ЗКПО, ЗОПБ, ЗЗО, ЗЗЛД, ЗМИП и ЗМФТ, Закона за задълженията и договорите; Наказателно процесуалния кодекс.	Хартиени и технически носител	Първични документи-носители на инф-я за регистриране за първи път на стопанска операция; Вторични документи, носители на преобразувана инф-я-обобщена или диференцирана-Платежен документ за извършено плащане, фактури, искания за разход, разходни ордери	Сч. Инф-я се съхранява на хартиен и/или на технически носител в следните срокове: Ведомости за заплати -50 години, считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят; счетоводни регистри и финансове отчети, вкл. Документи за данъчен контрол, одит и последващи финансови инспекции-10 год. считано от 1 януари на отчетния период,	Високо/ В шкафове с ключалки.В работни помещения; Лична парола за достъп; Сървър; СОТ

	адрес; данни за професионалната дейност на лицето и целта и характера на участието на лицето в деловите взаимоотношения чрез използване на документи; Идентифициране на юридически лица съгл. ЗМИП: оригинал или нотариално заверено копие на официално извлечение от съответния регистър за актуалното им състояние и заверено копие от учредителния договор, учредителния акт или от друг документ; наименованието; правноорганизационната форма; седалището; адреса на управление; адреса за кореспонденция; актуалния предмет на дейност или целта и характера на деловите взаимоотношения или на случайната операция, или сделка; срока на съществуване; контролните органи, органите на управление и представителство; вида и състава на колективния орган на управление; основното място на търговска дейност.				следващ отчетния период, за който се отнасят; всички останали носители на сч. инф-я-3 год., считано от 1 януари на отчетния период, следващ отчетния период, за който се отнасят. Лечебното заведение съхраняват за срок 5 години всички събрани и изготвени по реда на ЗМИП и ППЗМИП документи, данни и информация. Документите, получавани, изготвяни и обработвани от дирекция "Финансово разузнаване" на Държавна агенция "Национална сигурност" по реда и за целите на ЗМИП и ППЗМИП, се съхраняват от дирекцията за срок 10 години, освен ако със закон е предвиден по-дълъг срок за съхранение.	

Регистър „Деловодство” Отговорник: технически секретар	Имена на служители, ЕГН-та, наименования на фирми-контрагенти и институции	работата по регистрацията, движението и съхранението на входяща, изходяща и вътрешна документация в МБАЛ	Хартиен, електронен носител	Заповеди, графици, УП-2, УП-3, документи за входиране от Личен състав; вътрешни доклади; договори-граждански, доставка, наем, услуга, дарение, мед. д-ст; писма за припознаване, преписки –МВР, Съд, Прокуратура, РУ-Социално подпомагане, вътрешна кореспонденция	според номенклатурата на заведените документи	Средно/ В шкафове.В работни помещения; Сървър; СОТ
Регистър „ Обществени поръчки” Отговорник: юрисконсулт	наименования на фирми-контрагенти	ЗОП, ППЗОП, ТЗ, ЗЗД	Хартиен, електронен носител		До изтичане на срока за подаване на предложения та цялата документация по подготовката на процедурата се съхранява при отговорника по изготвянето; по време на работата на Комисията цялата документация заедно с постъпилите предложения се съхранява от председателя на Комисията; окомплектованите досиета на ОП се съхраняват от юрисконсулта; след изпълнение на договора досиетата се архивират за срок от пет години, като в описа се посочва датата на изпълнение	

					на договора или от датата на прекратяване на процедурата	
Регистър на архива Отговорник: архивар	Всякакви документи и документация, която МБАЛ е използвала в процеса на дейността на си	Закон за държавния архив	Хартиен носител	Формите за регистриране и отчитане на приетите документи в учрежденския архив са регистрите на постъпленията по образец и списъците, с които се приемат документите в учрежденския архив по образец. Списъците се изготвят от предаващите структурни звена. Общоадминистративн и документи се поставят и съхраняват в твърди папки или в кутии. Твърдите папки и подвързаните томове се съхраняват във вертикално положение. Достъп до архивохранилищата има само длъжностното лице, отговарящо за съхраняването и използването на документите от архива, и в негово присъствие - лица, оторизирани да извършват контрол по опазването и съхраняването на документите.	След извършване на експертиза на ценността на документите при спазване разпоредбите на чл. 51 от ЗНАФ.	Средно/В работни помещения на метални рафтове; Общоадминист ративни документи се поставят и съхраняват в твърди папки или в кутии/кашони; СОТ

Регистър „Видеонаблюдение”	В този регистър се обработват само „обикновени” лични данни, както следва: Обикновени данни за физическа идентичност: запис на образ и звук.	Опазване живота и здравето на граждани, пациенти, работници/ служители, както и опазване имуществото на лечебното заведение. Данните, обработвани в този регистър служат за превантивна мярка за предотвратяване на престъпления в и около сградата на лечебното заведение, също така служат и за подпомагане на разследващите органи при събиране на доказателства при евентуално извършено престъпления в територията на обхвата на видеонаблюдение Данните в Регистър „Видеонаблюдение” се обработват на основание чл.6, т.1, б. „б” и „д” от Регламент (ЕС) 2016/679	Регистър „Видеонаблюдение” се съхранява в електронен вид, който представлява аудио и видео запис от съответната записваща техника.	Обработването на лични данни в него се извършва чрез автоматични средства посредством отдалечен достъп на служители на фирмата охранител	Срокът на съхранението на видеозаписи, генерирани от системата за видеонаблюдение, е 30 (трийсет) календарни дни, следващи датата на осъществяване на видеозаписа.	Високо/ Фирмата охранител се задължава при извършване на денонощното наблюдение на сигнала от системата за видеонаблюдение да спазва стриктно правилата на Закона за защита на личните данни, на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27.04.2016 г. и на Закона за частната охранителна дейност

§ 8. Настоящите Вътрешни правила са допълнени в частта им Регистър „Видеонаблюдение” към Приложение №1 със Заповед №ОА-58-1/03.06.2019 г.