

ПРИМЕРНА ИНСТРУКЦИЯ

УТВЪРЖДАВАМ:

(ПОДПИС И ПЕЧАТ)

ВЪТРЕШНИ ПРАВИЛА ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ В ЛЕЧЕБНО ЗАВЕДЕНИЕ

I. ПРАВНО ОСНОВАНИЕ

Чл. 1. Настоящите правила се издават на основание Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета (Регламента) и Закона за защита на личните данни (ЗЗЛД).

II. ПРЕДМЕТ И ЦЕЛ НА ПРАВИЛАТА

Чл. 2. С настоящите правила се определят редът, начинът, основните принципи по отношение на защитата на физическите лица във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни в дейността на

.....
(*наименование на лечебното заведение, ЕИК, адрес,*)

в качеството му на администратор на лични данни (АЛД) по смисъла на Регламента и ЗЗЛД.

Чл. 3. (1) Настоящите правила имат за цел да регламентират:

а) механизмите на водене, поддържане и защита на личните данни на персонала и пациентите, обработвани от администратора на лични данни;

б) задълженията на оправомощените лица, обработващи личните данни и тяхната отговорност при неизпълнение на тези задължения;

в) необходимите технически и организационни мерки за защита личните данни 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).

(2) Основните принципи при обработването и защитата на личните данни, съгласно Регламента, и които АЛД следва да спазва, са личните данни да бъдат:

а) законосъобразно, добросъвестно и по прозрачен начин обработвани по отношение на субекта на данните („**законосъобразност, добросъвестност и прозрачност**“);

б) 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 от Регламента, за несъвместимо с първоначалните цели („**ограничение на целите**“);

в) подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват („**свеждане на данните до минимум**“);

г) точни и при необходимост да бъдат поддържани в актуален вид; трябва да 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**“);

д) 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 от Регламента, при условие, че бъдат приложени подходящите технически и организационни мерки, предвидени в Регламента с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

е) 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 или организационни мерки („цялостност и поверителност“);

(3) АЛД и обработващият лични данни носят отговорност и са в състояние да докажат спазването на принципите по ал. 2 („отчетност“).

III. РЕГИСТРИ И ДЕЙНОСТИ ПО ОБРАБОТВАНЕ

Чл. 4. (1) На основание и със съдържание, отразено в чл. 30 от Регламента, АЛД, респективно обработващият лични данни (*при наличие*), води (*водят*) регистри на дейностите по обработване на лични данни на физическите лица. Обработващият лични данни и всяко лице, действащо под ръководството на АЛД или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването не се изисква от правото на Европейския съюз или правото на държава членка

Обработването се извършва на адрес:.....

Личните данни на физическите лица се събират и обработват с оглед:

1. сключени трудови/граждански договори;
2. оказване на медицински услуги на пациенти;
3. други цели:.....

(2) АЛД води следните регистри:

1. Регистър „Персонал”
2. Регистър „Пациенти”
3. Регистър „Заявления и жалби”.
4. **Видеонаблюдение** (*при наличие следва да бъде описано отделно*)

Чл. 5. (1) Общо описание на Регистър „Персонал“ и дейности по обработване:

1. В регистъра се обработват лични данни на служителите и изпълнителите по граждански договори, сключени с физически лица, с оглед: (1) индивидуализиране на трудови, служебни и граждански правоотношения; (2) изпълнение на нормативните изисквания на Кодекса на труда, Кодекса за социално осигуряване, Закона за счетоводството и др.; (3) използване на събраните данни за съответните лица за служебни цели, като (но не само): за всички дейности, свързани със съществуване, изменение и прекратяване на трудовите и граждански 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); за установяване на връзка с лицето по телефон, за изпращане на кореспонденция, отнасяща се до изпълнение на задълженията му по трудови или граждански договори; за водене на счетоводна отчетност относно възнагражденията и разходите за командировки на посочените по-горе лица по трудови и служебни правоотношения и граждански договори.

2. Категории лични данни: (1) физическа идентичност: име, ЕГН, адрес, паспортни данни, месторождение, телефон, адрес на електронна поща; (2) социална идентичност: образование,

трудова дейност, квалификация (3) медицинско свидетелство и свидетелство за съдимост при започване на работа (4) болнични листа.

3. Източници от които се събират данните: от физическите лица, за които се отнасят данните, с тяхното изрично съгласие.

(2) Технологично описание на регистъра:

1. Носители на данни - данните в регистъра се обработват на хартиен и технически носител (компютър).

След като се съберат и обработят данните на хартиен носител се класифицират в отделни досиета, които се съхраняват в

Данните на технически носител се съхраняват и обработват само на компютър, който се помещава в с контрол на достъпа.

2. Технология на обработване - данните в регистъра се предоставят от физическите лица при кандидатстване за работа по трудов договор или при сключване на граждански договор с физическо лице и се въвеждат директно в трудови или граждански договори, допълнителни споразумения, както и в други документи, удостоверяващи трудов стаж, служебни бележки, справки, удостоверения, кореспонденция и др.

3. Срок на съхранение - всички данни в регистър „Персонал“ се съхраняват за срок от 5 години след прекратяване на трудовия или гражданския договор със съответното физическо лице, с изключение на данните от счетоводни ведомости, които съгласно изискването на закона трябва да се съхраняват за срок от 50 години.

4. Предоставени услуги – данни от регистър „Персонал“ не се предоставят извън целите на тяхната обработка, с изключение: (1) по изрично искане и нареждане на лицето или на неговите наследници в срока за съхранение; (2) по разпореждане на закона - на държавни институции в изпълнение на служебните им задължения (данъчни служители, служители на НОИ, Инспекция по труда, полиция и др. подобни); (3) при съдебни дела - на процесуален представител или директно на съда при стриктно спазване на разпоредбите на закона и настоящите правила.

(3) Длъжности, свързани с обработването и защитата на лични данни от регистър „Персонал“ и описание на техните права и задължения:

1. Данните в регистър „Персонал“ се обработват от:
(наименование, ЕИК и адрес ако е възложено на външна фирма като „обработващ ЛД“)

2. Правата и задълженията на обработващия са уредени с:
(длъжностна характеристика или договор)

(4) Оценката на въздействието върху защитата на данните за целите на регистър „Персонал“ се извършва за да се оценят конкретната вероятност и тежестта на високия риск, като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска. Посочената оценка на въздействието включва по-специално предвидените мерки, гаранции и механизми за ограничаване на този риск, с които се осигурява защитата на личните данни и се доказва съответствието с Регламента.

Чл.6. (1) Общо описание на Регистър „Пациенти“ и дейности по обработване:

1. В регистъра се обработват лични данни на пациентите с оглед: лечението им, включително консултиране, диагностициране, преценка за вида и обема на лечебните дейности, профилактика, превенция и всички други дейности представляващи добра дентална практика.

2. Категории лични данни: (1) физическа идентичност: име, ЕГН, адрес, паспортни данни, месторождение, телефон, адрес на електронна поща; (2) социална идентичност: образование, трудова дейност, квалификация (3) данни за здравословното състояние на пациента, представляващи т.нар. чувствителни данни.

3. Източници от които се събират данните: (1) от пациентите - физически лица, за които се отнасят данните, с тяхното изрично информирано съгласие, лично, или в определени случаи със съгласието на техен представител (2) от обществено достъпни източници - НЗОК, НОИ, НАП и др. подобни.

(2) Технологично описание на регистъра:

1. Носители на данни - данните в регистъра се обработват на хартиен и технически носител (компютър). След като се съберат и обработят данните на хартиен носител се класифицират в отделни досиета, които се съхраняват в

Данните на технически носител се обработват само на компютър, който се помещава в с контрол на достъпа.

Данните могат да се съхраняват и обработват и чрез услугата в WEB-базираната програмна система на

2. Технология на обработване - данните в регистъра се предоставят от пациентите и се въвеждат в тяхно лично пациентско досие, а когато е необходимо по искане на пациента или в изпълнение на законови разпоредби - се вписват и в съответните медицински документи.

3. Срок на съхранение - всички данни в регистър „Пациенти“ се съхраняват за срок, определен с нормативен акт, или ако липсва такъв срок – най-късно до 5 години от датата, на която лицето е престанало да бъде пациент на лечебното заведение (включително и при смърт).

В случай, че пациентът поиска данните му да бъдат заличени преди изтичането на предвидените 5 години за съхранението им, данните на пациента се заличават в 30-дневен срок от подаване на искането, освен ако това не е допустимо по закон или са налице правни претенции.

4. Предоставени услуги – данни от регистър „Пациенти“ не се предоставят извън целите на тяхната обработка, с изключение: (1) по изрично искане и нареждане на лицето или на неговите наследници в срока за съхранение; (2) по разпореждане на закона - на държавни институции в изпълнение на служебните им задължения (НЗОК, НОИ, ИА “Медицински одит“, Инспекция по труда, НАП, органи на съдебната власт, полиция и др.).

На други лечебни заведения данните на пациента се предоставят само с негово информирано съгласие и/или в съответствие с разпоредбите на Закона за здравето и други закони, съдържащи императивни разпоредби.

(3) Длъжности, свързани с обработването и защитата на лични данни от регистър „Пациенти“ и описание на техните права и задължения:

1. Данните в регистър „Пациенти“ се обработват от:

2. Правата и задълженията на обработващия са уредени с:

(длъжностна характеристика или договор)

(4) Оценката на въздействието върху защитата на данните за целите на регистър „Пациенти“, се извършва за да се оценят конкретната вероятност и тежестта на високия риск, като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска. Посочената оценка на въздействието включва по-специално предвидените мерки, гаранции и механизми за ограничаване на този риск, с които се осигурява защитата на личните данни и се доказва съответствието с Регламента.

Чл. 7. (1) Общо описание на Регистър „Заявления и жалби“ и дейности по обработване:

1. В регистъра се обработват лични данни на лица, които са подали заявления и жалби, включително при и по повод събирането и обработването на лични данни.

Личните данни се събират от предоставените от лицата заявления, жалби и др. подобни.

2. Категории лични данни: (1) физическа идентичност: име, ЕГН, адрес, телефон, адрес на електронна поща; (2) други данни: с оглед на конкретния случай – данни, които са вписани от самото лице или в представените от него документи

3. Източници от които се събират данните: от физическите лица, с тяхното изрично съгласие или съгласно изискванията на приложимия закон.

(2) Технологично описание на регистъра:

1. Носители на данни - данните в регистъра се обработват на хартиен и технически носител (компютър).

2. Технология на обработване:

След като се съберат и обработят данните на хартиен носител се класифицират в отделни досиета, които стоят в отделен шкаф с контрол на достъпа.

Данните на технически носител се съхраняват и обработват само на компютър с контрол на достъпа.

Данните се използват за воденето на кореспонденция, подготовка, разглеждане на съответната преписка и изпращане на отговор до подателя й.

3. Срок на съхранение - всички данни в регистър „Заявления и жалби“ се съхраняват за срок от 5 години след приключване на преписката, освен ако в закон не е предвиден друг срок.

4. Предоставени услуги – данни от регистър „Заявления и жалби“ не се предоставят извън целите на тяхната обработка, с изключение: (1) по изрично искане и нареждане на лицето, (2) по разпореждане на закона - на държавни институции в изпълнение на служебните им задължения (данъчни служители, служители на НОИ, Инспекция по труда, полиция и др. подобни) (3) при съдебни дела - на процесуален представител или директно на съда.

(3) Длъжности, свързани с обработването и защитата на лични данни от регистър „Заявления и жалби“ и описание на техните права и задължения:

1. Данните в регистър „Заявления и жалби“ се обработват от:

.....

2. Правата и задълженията на обработващите лични данни са уредени с:

.....

(длъжностна характеристика или договор)

(4) Оценката на въздействието се извършва периодично на всеки две години или при промяна на характера на обработваните лични данни и броя на засегнатите физически лица.

IV. МЕРКИ ЗА ЗАЩИТА ПРИ ОБРАБОТВАНЕ НА ЛИЧНИТЕ ДАННИ

Чл. 8. (1) Настоящите мерки регламентират и гарантират в подходяща степен сигурност и поверителност на личните данни, включително за предотвратяване на непозволен достъп до лични данни и до оборудване за тяхното обработване или за предотвратяване на използването им.

(2) Техническите и организационни мерки за защита трябва да:

-отхвърлят достъпа на неоторизирани лица до оборудването за обработка на данни – контрол на достъпа до оборудване;

-предотвратяват неоторизираното четене, копиране, промяна или унищожаване на информационни носители – контрол на информационните носители;

-предотвратяват неоторизираното добавяне, въвеждане, преглеждане, промяна или заличаване на съхранени лични данни – контрол по съхраняването;

-предотвратяват използването на личните данни от неоторизирани лица, използващи комуникационно оборудване за данни – контрол на потребителите;

-гарантират, че лицата, които са оторизирани да ползват система за автоматизирана обработка на данни, имат достъп само до данните, включени в обхвата на техния достъп –

контрол на достъпа до данни;

-осигуряват възможността за проверка и установяване до кои органи са били или могат да бъдат изпратени или предоставени личните данни чрез използване на комуникационно оборудване за данни – контрол на комуникациите;

-осигуряват възможност за последваща проверка и установяване какви лични данни са въведени в системите за автоматизирана обработка на данни, кога и от кого са въведени данните – контрол на въвеждане;

-предотвратяват неототоризирано четене, копиране, промяна или изтриване на лични данни при трансфер на лични данни или превозване на носители на данни – контрол при транспортиране;

-осигуряват възможност инсталираните системи да могат да се възстановят в случаи на прекъсване на функционирането – възстановяване;

-осигуряват правилното функциониране на системата, докладване на появата на грешки във функциите (надеждност) и гарантират, че съхранените данни не могат да бъдат повредени чрез неправилно функциониране на системата – интегритет.

(3) При автоматичното обработване на лични данни се осъществяват подходящи технически мерки за защита срещу:

-неототоризирано четене, възпроизвеждане, промяна или премахване на носителя на данните;

-неототоризирано въвеждане, промяна или заличаване на съхранени лични данни;

-неототоризирано използване на системите за лични данни чрез средства за пренос на данни;

-неототоризиран достъп до лични данни.

(4) Автоматичното обработване на данни се осъществява след въвеждане на потребителско име и парола в системата.

(5) АЛД, както и всички лица с достъп, работещи по негово ръководство или това на обработващия лични данни, отговарят за прилагане и спазване на мерките за защита.

V. УВЕДОМЯВАНЕ НА КЗЛД ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл. 9 (1) В случай на нарушение на сигурността на личните данни АЛД, без ненужно забавяне и когато това е осъществимо — **не по-късно от 72 часа** след като е разбрал за него, уведомява за нарушението на сигурността на личните данни КЗЛД, освен когато не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

(2) Обработващият лични данни уведомява администратора без ненужно забавяне след като узнае за нарушаване на сигурността на лични данни.

(3) В уведомлението се съдържа най-малко следното:

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

б) посочване на името и координатите за връзка на длъжностното/отговорното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) 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) Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на надзорния орган - Комисията за защита на личните данни - да провери дали е спазен закона.

VI. СЪОБЩАВАНЕ НА СУБЕКТА НА ДАННИТЕ ЗА НАРУШЕНИЕ НА СИГУРНОСТТА НА ЛИЧНИТЕ ДАННИ

Чл.10 (1) Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът, без ненужно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.

(2) В съобщението до субекта на данните, посочено в ал.1, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени по-горе в раздел V, чл. 9 ал. 3 букви б), в) и г).

(3) Съобщение не се изисква, ако някое от следните условия е изпълнено:

а) 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 мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

б) администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни;

в) 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, КЗЛД може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията по ал. 3.

VII. ДЕЙСТВИЯ ЗА ЗАЩИТА ПРИ АВАРИИ, ПРОИЗШЕСТВИЯ И БЕДСТВИЯ (ПОЖАР, НАВОДНЕНИЕ И ДР.)

Чл. 11 (1) При възникване и установяване на инцидент с наличните ресурси се вземат мерки за ограничаване въздействието върху регистрите, доколкото това е възможно.

(2) За инцидентите се води дневник, в който задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализ на инцидента, в дневника се вписват последствията от инцидента и мерките, които са предприети за отстраняването им.

(3) В предвидените в Регламента и ЗЗЛД случаи за инцидента се уведомява надзорния орган – Комисията за защита на личните данни.

VIII. ПРАВА ЗА ДОСТЪП НА ЛИЦАТА ДО ЛИЧНИТЕ ИМ ДАННИ, ПРАВОТО „ДА БЪДЕШ ЗАБРАВЕН”, ПРАВО НА ПРЕНОСИМОСТ, ПРАВО НА ВЪЗРАЖЕНИЕ

Чл. 12. (1) Заетите по трудови и граждански правоотношения, както и пациентите, имат право на достъп до личните си данни, право на коригиране на личните им данни, право на

изтриване /правото „да бъдеш забравен“/, право на ограничаване на обработването, право на преносимост на данните и право на възражение.

(2) Лицата, които желаят да упражнят горепосочените си права подават писмено заявление до АЛД лично или чрез упълномощено лице. Подаването на заявление по електронен път става чрез електронен подпис по реда на ЗЗЛД.

(3) Заявлението съдържа име на лицето и други данни, които го идентифицират – тези, които ЗЗЛД изрично допуска да бъдат посочени, описание на искането, предпочитана форма за предоставяне достъпа до лични данни, подпис, дата и адрес на кореспонденцията; пълномощно – когато заявлението се подава от упълномощено лице. Заявлението се завежда в общия входящ регистър на администратора.

(4) Достъп до данните на лицето се осигурява под формата на:

1. устна справка;
2. писмена справка;
3. преглед на данните от самото лице или упълномощено от него такова;
4. предоставяне на копие от исканата информация.

(5) При подаване на искане за осигуряване на достъп администраторът на лични данни разглежда заявлението за достъп и/или разпорежда да се осигури искания от лицето достъп в предпочитаната от заявителя форма. Срокът за разглеждане на заявлението и произнасяне по него е 14-дневен от деня на подаване на искането, съответно 30-дневен, когато е необходимо повече време за събиране личните данни на лицето с оглед възможни затруднения в дейността на администратора. Решението се съобщава писмено на заявителя лично срещу подпис или по пощата с обратна разписка. Когато данните не съществуват или не могат да бъдат предоставени на определено правно основание, на заявителя се отказва достъп до тях с мотивирано решение. Отказът за предоставяне достъп може се обжалва от лицето пред посочения в писмото орган и срок.

(6) Достъп до личните данни на лицата, съдържащи се на технически носител има само администратора на лични данни, а в негово отсъствие и когато тези данни се отнасят до възнагражденията на лицата, достъп до тях има изрично упълномощено от администратора на лични данни лице.

(7) По другите заявени искания, съгласно посоченото в ал (1) на този член, АЛД се произнася в максимално кратки срокове, съгласно разпоредбите на Регламента и ЗЗЛД.

Чл. 13. Освен от администратора на лични данни, правомерен достъп до определени категории лични данни могат да имат и лица, определени от него с изрична заповед. Администраторът носи отговорност за избора на тези лица.

Чл. 14. (1) Никое трето лице няма право на достъп до регистрите с лични данни на лицата, освен в случаите, когато се предоставя информация, която е изисквана на основание на закона и по надлежен път от Комисията за защита на личните данни, от съдебната власт или от друг орган на държавна власт.

(2) При условия, налагащи прехвърляне на регистрите за лични данни от един АЛД към друг, предаването на регистъра се извършва по предвидения от Регламента и ЗЗЛД ред и след разрешение на Комисията за защита на лични данни.

IX. ДРУГИ УСЛОВИЯ

Чл. 15. При внедряване на нов програмен продукт за обработване на лични данни се извършва тестване на възможностите на продукта, с оглед спазване изискванията на Регламента и ЗЗЛД за осигуряване максималната защита на личните данни от правомерен достъп, загубване, повреждане или унищожаване.

Чл. 16. При неизпълнение на задълженията им, вменени с разпоредбите на Регламента, ЗЗЛД и настоящите вътрешни правила, на съответните лица, обработващи лични данни под ръководството на АЛД и/или при обработващия лични данни, се налагат дисциплинарни наказания по Кодекса на труда или административни наказания, когато нарушението е констатирано и установено от надлежен орган, а когато са налице причинени вреди - им се търси отговорност по съответния приложим закон.

Чл.17. Адресът, на който се приемат молби и заявления е
или на електронен адрес:

Чл. 18. Контролът върху дейностите по обработване на лични данни се осъществява от АЛД.

Чл. 19. За неуредените с тези правила въпроси се прилагат разпоредбите на Регламента и ЗЗЛД.

Х. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 20. По смисъла на Регламент (ЕС) 2016/679 и настоящите правила:

1. „**Лични данни**“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата и умствената, икономическата, културната или социалната идентичност на това физическо лице.

2. „**Администратор на лични данни**“ означава компетентният орган, който сам или съвместно с други органи определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Европейския съюз или правото на Република България, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Европейския съюз или в националното законодателство

3. „**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, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на осигуряване на достъп до данните, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

4. „**Обработващ лични данни**“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

5. „**Регистър с лични данни**“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип.

6. „**Лице с достъп до данни**“ е всяко лице, действащо под ръководството на администратора или на обработващия, което има достъп до лични данни, може да ги обработва само по указание на администратора, освен ако в закон е предвидено друго.

7. „**Предоставяне на лични данни**“ са действия по цялостно или частично пренасяне на лични данни от един администратор към друг или към трето лице на територията на страната или извън нея.

8. „Носител на лични данни“ е физически обект, на който могат да се запишат данни или могат да се възстановят от същия.

9. „Поверителност“ е изискване за неразкриване на личните данни на неоторизирани лица в процеса на тяхното обработване.

10 „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.

11. „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.

12. „ЗЗЛД“ е Закон за защита на личните данни.

13. „КЗЛД“ е Комисия за защита на личните данни.

14. „Регламент“ е Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета.

Чл. 21. Настоящите правила се прилагат от 25.05.2018 г.

Чл. 22. Неразделна част от настоящите правила са:

Приложение № 1. Декларация за поверителност.

Приложение № 2. Декларация за съгласие (*Персонал*).

Приложение № 3. Декларация за съгласие (*Пациент*).

Приложение № 4. Декларация за съгласие на родител/настойник.

Приложение № 5. Заявление за достъп до лични данни.

Приложение № 6. Заявление за преносимост на лични данни.

Приложение № 7. Заявление за коригиране на лични данни.

Приложение № 8. Заявление за заличаване на лични данни.

Приложение № 9. Заявление за ограничаване на обработването на лични данни.

ДЕКЛАРАЦИЯ
за поверителност

Долуподписаният/ата
в качеството си на
(*длъжност/позиция*)

на основание разпоредбите за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета, Закона за защита на личните данни и вътрешните правила на администратора на лични данни:.....

ДЕКЛАРИРАМ:

1. Запознат/а съм с:

- нормативната уредба в областта на защитата на личните данни;
- политиката и вътрешните правила за защита на личните данни на администратора на лични данни,
- опасностите за личните данни, обработвани от администратора на лични данни.

2. Поемам задължения за:

- несподеляне на критична информация между персонала (например идентификатори, пароли за достъп и т.н.);
- неразгласяване на лични данни, до които съм получил/а достъп при и по повод изпълнение на задълженията си, ако това не е предвидено изрично в закон или не застрашава живота и здравето на физическото лице.

Дата:.....

ДЕКЛАРАТОР:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 2.

(ПЕРСОНАЛ)

ДЕКЛАРАЦИЯ

Долуподписаният/ата
в качеството си на
(длъжност/позиция)

ДЕКЛАРИРАМ:

Съгласен/а съм администраторът на лични данни: да обработва личните ми данни, съгласно изискванията на Регламент (ЕС) 2016/679 и Закона за защита на личните данни. Предоставям доброволно личните си данни: три имена, ЕГН, място на раждане, образование, адрес, телефон, имейл за контакт, трудова история, здравословно състояние, имена на деца и ЕГН на децата /в случай че има/.

Запознат/а съм с:

– целта и средствата на обработка на личните данни – за изпълнение на трудовия ми договор и по законоустановените изисквания на Кодекса на труда, Кодекса за социалното осигуряване, Закона за здравното осигуряване, Закона за данъка върху доходите на физическите лица;

–доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;

–правото на достъп, на коригиране и на изтриване на събраните данни;

–получателите или категориите получатели, на които могат да бъдат разкрити данните – НОИ, НАП, МВР, данъчни власти, НЗОК и други органи и власти по силата на законоустановено изискване.

С настоящото давам изричното си съгласие личните ми данни да бъдат съхранявани в базата данни на администратора на лични данни и да бъдат обработвани от него за срока на действие на трудовия ми договор и пет години след това, както и в законоустановените други задължителни срокове съгласно приложимото законодателство. С подписване на тази декларация - съгласие заявявам, че съм предоставил личните си данни доброволно на администратора на лични данни.

Декларирам, че съм уведомен/а за:

– последиците от отказ за предоставяне на лични данни биха довели до невъзможност да бъде сключен и изпълнен трудовия ми договор;

– мога да упражня правото си на достъп и коригиране на личните ми данни на адреса на управление на работодателя ми;

– имам правото да бъдат заличени личните ми данни;

– имам правото да възразя срещу обработване на предоставените мои лични данни за целите на директния маркетинг, както и да бъда уведомен/а преди личните ми данни да бъдат разкрити за първи път на трети лица или използвани от тяхно име за целите на директния маркетинг и да възразя срещу такова разкриване или използване.

Дата:.....

ДЕКЛАРАТОР:.....

гр./с/.....

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 3.

(ПАЦИЕНТ)

ДЕКЛАРАЦИЯ

Долуподписаният/ата
ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

ДЕКЛАРИРАМ:

Съгласен/а съм администраторът на лични данни:
....., да обработва личните ми данни, съгласно
изискванията на Регламент (ЕС) 2016/679 и Закона за защита на личните данни, и предоставям
доброволно личните си данни.

Запознат/а съм с информацията и правата си, включително (но не само) и с:

- наименованието, седалището и адреса на администратора на лични данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото да оттегля по всяко време настоящето съгласие;
- правото на достъп, на коригиране и на изтриване на събраните данни;
- категории на личните данни, които ще се обработват, като съм уведомен/а, че тези данни са „чувствителни“:

.....
- целта на обработването на личните данни:

.....
- средствата на обработването на личните данни :

.....
- срока на обработването на личните данни:

.....
- получателите или категориите получатели, на които могат да бъдат разкрити личните данни:.....

- други условия:

Дата:.....

ДЕКЛАРАТОР:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 4.
(РОДИТЕЛ/НАСТОЙНИК)

ДЕКЛАРАЦИЯ

Долуподписаният/ата
ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

в качеството си на родител/настойник на

.....

ДЕКЛАРИРАМ:

Съгласен/а съм администраторът на лични данни:

.....
да обработва личните данни, на лицето, за което давам съгласие, съгласно изискванията на Регламент (ЕС) 2016/679 и Закона за защита на личните данни.

Запознат/а съм с информацията и правата си, включително (но не само) и с:

- наименованието, седалището и адреса на администратора на лични данни;
- доброволния характер на предоставянето на данните и последиците от отказа за предоставянето им;
- правото да оттегля по всяко време настоящето съгласие;
- правото на достъп, на коригиране и на изтриване на събраните данни;
- категории на личните данни, които ще се обработват, като съм уведомен/а, че тези данни са „чувствителни“;

.....
- целта на обработването на личните данни:

.....
- средствата на обработването на личните данни :

.....
- срока на обработването на личните данни:

.....
- получателите или категориите получатели, на които могат да бъдат разкрити личните данни:.....

.....
- други условия:

Дата:.....

ДЕКЛАРАТОР:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 5.

ДО

Адрес:

З А Я В Л Е Н И Е ЗА ДОСТЪП ДО ЛИЧНИ ДАННИ

Долуподписаният/ата,

ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

На г., след извършена справка в
установих, че личните ми данни са обработвани от Вас като администратор на лични данни с
цел

Моля, на основание Регламент (ЕС) 2016/679, Закона за защита на лични данни и вътрешните
Ви правила да ми бъде предоставена информация относно личните ми данни, съхранявани от Вас, а
именно:

.....
.....

Желая да получа исканата от мен информация в следната форма:

.....

(необходимото се изписва)

- преглед на информация;
- устна справка;
- писмена справка;
- копия на технически носител;
- по електронен път.

Приложение:

1. Документ за самоличност (*представя се само за идентификация, но не се снима*).

2.

Дата:.....

ЗАЯВИТЕЛ:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 6.

ДО

Адрес:

З А Я В Л Е Н И Е

ЗА ПРЕНОСИМОСТ НА ЛИЧНИ ДАННИ

Долуподписаният/ата,
ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

На г., след извършена справка в
установих, че личните ми данни са обработвани от Вас като администратор на лични данни с
цел

Бих желал/а да упражня правата си по Регламент (ЕС) 2016/679, Закона за защита на лични
данни и вътрешните Ви правила като АЛД, за да получа на ръка съответните документи,
съдържащи мои лични данни, и които съм Ви предоставил/а за медицински цели в качеството
Ви на администратор на лични данни, в структуриран, широко използван и пригоден за
машинно четене формат.

Ако е технически осъществимо, желая и моля да извършите пряко прехвърляне на личните
ми данни към

.....
(ако има такова искане, посочва се наименованието на другия АЛД, ЕИК, адрес за
кореспонденция)

Приложение:

1. Документ за самоличност (*представя се само за идентификация, но не се снима*).

.....

Дата:.....

ЗАЯВИТЕЛ:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 7.

ДО

Адрес:

З А Я В Л Е Н И Е

ЗА КОРИГИРАНЕ НА ЛИЧНИ ДАННИ

Долуподписаният/ата
ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

На г., след извършена справка в
установих, че личните ми данни са обработвани от Вас като администратор на лични данни с
цел

.....
Считам, че така представените мои лични данни има:

непълнота

неточност

грешка

поради което бих желал/а да упражня правата си по Регламент (ЕС) 2016/679, Закона за
защита на лични данни и вътрешните Ви правила като АЛД, за коригиране/допълване без
ненужно забавяне на личните данни, свързани с мен във Вашата система.

Приложение:

1. Документ за самоличност (*представя се само за идентификация, но не се снима*).

2.

Дата:.....

ЗАЯВИТЕЛ:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 8.

ДО

Адрес:

З А Я В Л Е Н И Е

ЗА ЗАЛИЧАВАНЕ НА ЛИЧНИ ДАННИ

Долуподписаният/ата

ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

На г., след извършена справка в установих, че личните ми данни са обработвани от Вас като администратор на лични данни с цел

Бих желал/а да упражня правата си по Регламент (ЕС) 2016/679, Закона за защита на лични данни и вътрешните Ви правила като АЛД, за изтриване/заличаване на свързаните с мен лични данни без ненужно забавяне във Вашата система на следните основания:

личните данни повече не са необходими за целите, за които са били събрани или обработвани;

оттеглям своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;

възразявам срещу обработването;

няма законни основания за обработването, които да имат преимущество;

личните данни са били обработвани незаконосъобразно;

личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Европейския съюз или правото на Република България;

личните данни са били събрани във връзка с предлагането на услуги на информационното общество.

Приложение:

1. Документ за самоличност (*представя се само за идентификация, но не се снима*).

2.

Дата:.....

ЗАЯВИТЕЛ:.....

гр./с/

(подпис и фамилия)

ПРИЛОЖЕНИЕ № 9.

ДО

Адрес:

З А Я В Л Е Н И Е

ЗА ОГРАНИЧАВАНЕ НА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Долуподписаният/ата
ЕГН/ЕНЧ.....

В случай, че се изисква и:

Л.К. №, издадена на г. от МВР гр.

или гражданин на

Паспорт.....издаден наг. от

с адрес за кореспонденция:

На г., след извършена справка в
установих, че личните ми данни са обработвани от Вас като администратор на лични данни с
цел

.....
Бих желал/а да упражня правата си по Регламент (ЕС) 2016/679, Закона за защита на лични
данни и вътрешните Ви правила като АЛД, за ограничаване на обработването на личните данни,
свързани с мен във Вашата система, на основание:

оспорвам точността на личните данни;

считам, че обработването е неправомерно, но не желая личните данни да бъдат изтрети, а
изисквам ограничаване на използването им;

считам, че Вие не се нуждаете повече от личните данни за целите на обработването;

възразявам срещу обработването.

Приложение:

1. Документ за самоличност (*представя се само за идентификация, но не се снима*).

2.

Дата:.....

ЗАЯВИТЕЛ:.....

гр./с/

(подпис и фамилия)