



## **ПРАВИЛА ЗА УПРАЖНЯВАНЕ ПРАВТА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ**

Настоящите правила („Правила“) определят условията и реда, по който физическите лица, чиито лични данни се обработват от „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД („Дружеството“), могат да упражнят правата си съгласно законодателството за защита на личните данни.

### **ЧАСТ I: ДЕФИНИЦИИ**

Изброените по-долу дефиниции имат следното значение:

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

„**Данни за здравословното състояние**“ означава лични данни, свързани с физическото или психическото здраве на физическо лице. Тези данни се ползват със специална защита, предвид техния чувствителен характер, и се обработват от медицински специалисти, обвързани от задължение за професионална тайна.

„**Приложимо законодателство**“ означава законодателство на Европейския съюз и на Република България, което е относимо към защитата на личните данни;

„**Профилиране**“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

„**Субект на данни**“ означава физическо лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

„**Регламент (ЕС) 2016/679**“ означава Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), обнародван в Официален вестник на Европейския съюз на 4 май 2016 г.

## **ЧАСТ II. ОБЩИ ПРИНЦИПИ**

1. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД обработва и защитава личните данни, събрани при изпълнение на дейността на Дружеството, честно, законосъобразно и в съответствие с целите, за които данните са събрани.
2. Служителите, които като част от трудовите си задължения обработват лични данни за целите на медицинското и административно обслужване на пациентите - физически лица, както и служителите, които обработват лични данни, свързани с човешките ресурси и контрагенти на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД, спазват следните принципи при обработване на лични данни:
  - 2.1. Личните данни се обработват законосъобразно и добросъвестно.
  - 2.2. Личните данни се събират за конкретни, точно определени и законосъобразни цели и не се обработват допълнително по начин, несъвместим с тези цели.
  - 2.3. Личните данни, които се събират и обработват при управление на човешките ресурси, са съотносими, свързани с и ненадхвърлящи целите, за които се обработват.
  - 2.4. Личните данни са точни и при необходимост се актуализират.
  - 2.5. Личните данни се заличават или коригират, когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват.
  - 2.6. Личните данни се поддържат във вид, който позволява идентифициране на съответните физически лица за период не по-дълъг от необходимия за целите, за които тези данни са събрани.
3. Служителите, които обработват лични данни, преминават първоначално и периодични обучения за поверителност на данните и се запознават с приложимото законодателство.
4. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД прилага всички подходящи технически и организационни мерки за гарантиране сигурността на личните данни, включително поемане на изрично задължение от служителите за професионална тайна и конфиденциалност.

## **ЧАСТ III. ПРАВА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ**

5. Субектите на лични данни имат следните права относно техните лични данни:
  - 5.1. Право на достъп;
  - 5.2. Право на коригиране;
  - 5.3. Право на преносимост на данните;
  - 5.4. Право на изтриване (право „да бъдеш забравен“);
  - 5.5. Право да се иска ограничаване на обработването;
  - 5.6. Право на възражение срещу обработването на лични данни;

5.7. Право на субекта на лични данни да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, независимо дали това обработване включва и профилиране.

### **Право на достъп**

6. При поискване „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД предоставя на субект на лични данни следната информация:

6.1. информация дали „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД обработва или не обработва личните данни на лицето;

6.2. копие от личните данни на лицето, които се обработват от „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД, освен когато същите се намират на носител/формат, съдържащ данни за трети лица, чиито съгласие е необходимо, за да бъдат същите предоставени на субекта на данните и

6.3. обяснение относно обработваните данни

7. Обяснението по чл. 6.3 включва следната информация относно обработваните от „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД лични данни:

7.1. целите на обработването;

7.2. категориите лични данни, които се обработват;

7.3. получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

7.4. когато е възможно, се посочва предвиденият срок, за който ще се съхраняват личните данни, а ако това е невъзможно се упоменават критериите, използвани за определянето на този срок;

7.5. съществуването на право да се изиска коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

7.6. правото на жалба до надзорен орган;

7.7. когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

7.8. съществуването на автоматизирано вземане на решения, независимо дали това обработване включва и профилиране, и информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните;

7.9. когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции във връзка с предаването.

8. Обяснението относно обработваните данни съдържа информацията, която „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД предоставя на субектите на данни посредством уведомления за поверителност.

9. При искане от субекта на лични данни, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД може да предостави копие от личните данни, които са в процес на обработване, освен когато същите се намират на носител/формат, съдържащ данни за трети лица, чиито съгласие е необходимо, за да бъдат същите предоставени на субекта на данните.

10. При предоставяне на копие от лични данни, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД не следва да разкрива следните категории данни:

- 10.1. лични данни на трети лица, освен ако същите не са изразили изричното си съгласие за това;
  - 10.2. данни, които представляват търговска тайна, интелектуална собственост или конфиденциална информация;
  - 10.3. друга информация, която е защитена съгласно приложимото законодателство.
11. Предоставянето на достъп на субекти на лични данни не може да влияе неблагоприятно върху правата и свободите на трети лица или да доведе до нарушаване на нормативно задължение на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД.

### **Право на коригиране**

12. Субекти на данни могат да поискат личните им данни, обработвани от „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД, да бъдат коригирани, в случай че последните са неточни или непълни.
13. При удовлетворено искане за коригиране на лични данни, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД уведомява другите получатели, на които са били разкрити данните (например държавни органи, доставчици на услуги), така че те да могат да отразяват измененията.

### **Право на изтриване (право „да бъдеш забравен“)**

14. При поискване, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД се задължава да изтрие лични данни, ако е налице някое от следните основания:
- 14.1. личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
  - 14.2. субектът на данните оттегля своето съгласие, на което се основава обработването на данните, и няма друго правно основание за обработването;
  - 14.3. субектът на данните възразява срещу обработването и няма законни основания за обработването, които да имат преимущество;
  - 14.4. субектът на данните възразява срещу обработването на лични данни за целите на директния маркетинг;
  - 14.5. личните данни са били обработвани незаконосъобразно;
  - 14.6. личните данни трябва да бъдат изтрети с цел спазването на правно задължение на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД;
  - 14.7. личните данни са били събрани във връзка с предлагането на услуги на информационното общество на деца по смисъла на член 8, параграф 1 от Регламент (ЕС) 2016/679.
15. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД не се задължава да изтрие личните данни, доколкото обработването е необходимо:
- 15.1. за упражняване на правото на свобода на изразяването и правото на информация;
  - 15.2. за спазване на правно задължение на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД;
  - 15.3. по причини от обществен интерес в областта на общественото здраве в съответствие с член 9, параграф 2, букви з) и и), както и член 9, параграф 3 от Регламент (ЕС) 2016/679;
  - 15.4. за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1 от Регламент (ЕС) 2016/679, доколкото съществува вероятност правото на изтриване да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или
  - 15.5. за установяването, упражняването или защитата на правни претенции.

## **Право на ограничаване на обработването**

16. Субектът на данните има право да изиска ограничаване на обработването, когато се прилага едно от следното:

16.1. точността на личните данни се оспорва от субекта на данните; ограничаването на обработването се прилага за срок, който позволява на администратора да провери точността на личните данни;

16.2. обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрети, а изисква вместо това ограничаване на използването им;

16.3. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;

16.4. субектът на данните е възразил срещу обработването на основание легитимния интерес на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД и тече проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.

17. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД може да обработва лични данни, чието обработване е ограничено, само за следните цели:

17.1. за съхранение на данните;

17.2. със съгласието на субекта на данните;

17.3. за установяването, упражняването или защитата на правни претенции;

17.4. за защита на правата на друго физическо лице; или

17.5. поради важни основания от обществен интерес.

18. Когато субект на данните е поискал ограничаване на обработването и е налице някое от основанията по чл. 18 по-горе, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД го информира преди отмяната на ограничаването на обработването.

## **Правото на преносимост на данните**

19. Субектът на данните има право да получи личните данни, които го касаят и които той е предоставил на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД, в структуриран, широко използван и пригоден за машинно четене формат.

20. При поискване тези данни могат да бъдат прехвърлени на друг администратор, посочен от субекта на лични данни, когато това е технически осъществимо

21. Субектът на личните данни може да упражни правото на преносимост в следните случаи:

21.1. обработването се извършва въз основа на съгласието на субекта на личните данни;

21.2. обработването се извършва въз основа на договорно задължение;

21.3. обработването се извършва по автоматизиран начин.

22. Правото на преносимост не може да влияе неблагоприятно върху правата и свободите на други лица.

## **Право на възражение**

23. Субектът на данните има право да възрази срещу обработване на негови лични данни от „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД, ако данните се обработват въз основа на едно от следните основания:

- 23.1. обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;
- 23.2. обработването е необходимо за цели, свързани с легитимните интереси на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД или на трета страна;
- 23.3. обработването на данни включва профилиране.
24. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за неговото продължаване, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

#### **Право на възражение срещу лични данни за целите на директния маркетинг**

25. Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработване на лични данни за тази цел, включително по отношение на профилиране, свързано с директния маркетинг.
26. Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява.

#### **Право на човешка намеса при автоматизирано вземане на решения**

27. В случаите, когато „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД взема автоматизирани индивидуални решения, независимо дали тези решения са взети с помощта на профилиране, които пораждат правни последствия за физически лица или ги засягат в значителна степен по подобен начин, тези лица могат да поискат преразглеждане на решението с човешка намеса, както и да изразят гледната си точка.
28. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД предоставя на физическите лица-обект на автоматизирано вземане на решения съществена информация относно използваната логика, както и относно значението и предвидените последствия от това обработване за лицето.

### **ЧАСТ IV.**

#### **РЕД ЗА УПРАЖНЯВАНЕ НА ПРАВАТА НА СУБЕКТИТЕ НА ЛИЧНИ ДАННИ**

29. Субектите на лични данни могат да упражнят правата съгласно тези Правила като подадат искане на упражняване на съответното право.
30. Искане за упражняване на правата на субектите на лични данни могат да бъдат подадени по следния начин:
- 30.1. По електронен път на следния имейл адрес: [info.sh@cardiacinstitute.bg](mailto:info.sh@cardiacinstitute.bg)
- 30.2. На място в „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД
- 30.3. По пощата - на адреса на „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД; гр. Шумен, ул. "Васил Априлов" № 63
31. Искането за упражняване на права, свързани със защитата на личните данни, следва да съдържа следната информация:
- 31.1. Идентификация на лицето – име и ЕГН (когато е приложимо);
- 31.2. Контакти за обратна връзка – адрес, телефон, електронна поща;

- 31.3. Искане – описание на искането и посочване на начина на получаване на отговор/кореспонденция по искането.
32. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД предоставя информация относно действията, предприети във връзка с искане за упражняване на правата на субектите, в срок от един месец от получаване на искането.
33. При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията от определено лице. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД информира лицето за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето.
34. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД не дължи отговори на искания, в случаите, когато дружеството не е в състояние да идентифицира субекта на данните.
35. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните, когато са налице основателни опасения във връзка със самоличността на физическото лице, което подава искане.
36. Когато исканията за упражняване на права на субектите са явно неоснователни или прекомерни, особено поради своята повторяемост, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД може да начисли разумна такса въз основа на административните разходи за предоставяне на информацията или да откаже да отговори на искането за упражняване на права. „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД преценява за всеки отделен случай дали дадено искане е явно неоснователно или прекомерно.
37. Като прекомерни ще бъдат отчитани всички искания на субектите на лични данни за упражняване на права, които вече са били напълно удовлетворени или които в голяма степен се припокриват с вече удовлетворени искания независимо от периодите и интервалите от време, изтекли между отделните искания, освен ако не е настъпила промяна в данните или други параметри на обработването след като първото искане е било удовлетворено. Например, в случай, че дадено искане е удовлетворено и последва ново искане за упражняване на същото право, като междуременно не е постъпила нова информация и не се обработват допълнителни лични данни на субекта, то въпросното искане ще бъде отчетено като прекомерно поради своята повторяемост. В такива случаи е възможно „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД да откаже да отговори на искането или да начисли разумна такса, базирана на административните разходи за уважаването му.
38. При отказ за предоставяне на достъп до лични данни, „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД аргументира отказа си информира субекта на данни за правото му да подаде жалба до Комисия по защита на личните данни (КЗЛД).
39. Когато искането е подадено с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни не е поискал друго.
40. Настоящите правила могат да се актуализират периодично, за да се отразят промените в практиките за защита на личните данни на лица, чиито данни се обработват от „Специализирана болница за активно лечение по кардиология Мадара“ ЕАД.