**РЕПУБЛИКА БЪЛГАРИЯ**
**Министерство на здравеопазването**
Регионална здравна инспекция Кюстендил

**УТВЪРДИЛ: /п/**

**Приложение № 2**

**Д-Р ЗЛАТКО ВЛИЧКОВ** **към Заповед №РД-11-348/23.1.2018 г.**

**ДИРЕКТОР НА РЗИ-КЮСТЕДИЛ**

# *Политика за защита на данните*

**Гр. Кюстендил, 2018 г.**

## 1.Въведение

В ежедневните си дейности Регионална здравна инспекция – Кюстендил (РЗИ-Кюстендил) използва различни данни за идентифицируеми лица, включително данни за:

- клиенти;
- настоящи, минали и бъдещи служители;
- договорни партньори;
- доставчици;
- други заинтересовани страни;

При събиране и използване на тези данни РЗИ-Кюстендил е обект на различни законодателни актове, които контролират начина, по който тези дейности могат да се извършват и предпазните мерки, които трябва да бъдат въведени за тяхната защита.

Целта на тази политика е да определи съответното законодателство и да опише стъпките, които Инспекцията предприема, за да гарантира, че е в съответствие с него.

Този контрол се прилага за всички служители и процеси, които работят с информационните системи на РЗИ-Кюстендил, включително ръководство, служители, клиенти, доставчици и други страни, които имат достъп до информационните системи и регистрите на Инспекцията.

## 2.Цел и основание на обработването на лични данни

РЗИ-Кюстендил събира и обработва лични данни, във връзка с осъществяване на официални правомощия, законови задължения и изпълнение на задачи с обществен интерес, за следните цели:

- надзор на заразните болести;
- държавен здравен контрол;
- регистрация и контрол на лечебни заведения за спазване на здравното законодателство;
- планиране, организиране, ръководство и контрол на медицинската експертиза;
- административно-наказателната дейност;
- за административни услуги;
- заявени лабораторни анализи и изпитвания;
- служебни и трудово-правни отношения;
- изпълнение на договори, по който РЗИ-Кюстендил е страна;
- проверка и отговор на жалби и сигнали.

## 3.Какви данни обработваме

Като Администратор на лични данни събираме и обработваме следната информация:

- име, презиме и фамилия;
- адрес;
- гражданство;

- идентификационен номер (ЕГН, ЛНЧ);
- документ за самоличност (данни за лична карта);
- данни за връзка (телефонен номер, електронен адрес);
- данни за здравословно състояние, включително генетични данни;
- диплома/професия ако е обявена от субекта на данни;
- данни на пълномощник (ако лицето се представлява от пълномощник)

Не събираме и не обработваме лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, данни за сексуалната ориентация на физически лица.

**4.Политика за защита на личните данни**

**4.1.Общ регламент относно защитата на данните**

Настоящата Политика се основава на изискванията на Регламент (ЕС) 2016/679 на ЕП и на Съвета от 27 април 2016 г. (GDPR), относно защитата на физическите лица във връзка с обработването на лични данни и свободното движение на такива.

Общият регламент е един от най-значимите законодателни актове, засягащи начина, по който РЗИ-Кюстендил като администратор на лични данни изпълнява дейностите по обработка на информацията, и спазва основните принципи и законовите разпоредби по събиране и обработване на лични данни и гарантира защитата им.

**4.2.Определения**

Като всяка информация, свързана с идентифицирано физическо лице в рамките на GDPR са изброени общо 26 определения, но най-фундаменталните определения по отношение на тази политика са следните:

- **„Лични данни"** са дефинирани или физическо лице, което може да бъде идентифицирано („субект на данни"); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;
- **„Обработване"** означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване*;*
- **„Администратор"** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това

обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

**5.Принципи, свързани с обработването на лични данни**

Съществуват редица фундаментални принципи, на които се основава GDPR, и които РЗИ-Кюстендил спазва при обработката на лични данни:

Те са както следва:

1. Личните данни са:

(а) обработвани законосъобразно, справедливо и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност");

(б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 89, параграф 1, за несъвместимо с първоначалните цели („ограничение на целите");

(в) подходящи, свързани със 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, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент 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");

2. Администраторът носи отговорност и е в състояние да докаже спазването на параграф 1 („отчетност").

РЗИ-Кюстендил ще гарантира, че отговаря на всички тези принципи както при обработката, която извършва в момента, така и като част от въвеждането на нови методи за обработка, като например нови информационни системи.

**6.Права на лицето**

Субектът на данните също има права съгласно GDPR. Те се състоят от:

1.Правото да бъде информиран - с настоящата политика информираме за обработваните от РЗИ-Кюстендил лични данни;

2.Правото на достъп - всеки субект на данни има право да получи потвърждение дали се обработват личните му данни, и ако това е така да получи достъп до тези данни след като направи заявка;

3.Правото на коригиране - ако субектът на данни информира аднинистратора, че личните му данни са неточни, непълни или са били променени, данните му ще бъдат коригирани и субектът на данните ще бъде информиран за това;

4.Правото за изтриване;

5.Правото да се ограничи обработката;

6.Правото на преносимост на данни;

7.Право на възражение;

8.Права във връзка с автоматизираното вземане на решения и профилиране;

9.Право на жалба до надзорен орган – в случай на установяване нарушение на законовите му права и интереси, субектът на данни има право на жалба до КЗЛД – гр.София 1592, бул. „Проф.Цветан Лазаров" № 2, www.cpdp.bg., тел. 02/9153518; e-mail: kzld@government.bg; kzld@cdpd.bg.

Всяко от тези права се подкрепя от подходящи процедури, прилагани от Инспекцията, които позволяват предприемането на необходимите действия в сроковете, посочени в GDPR.

Тези срокове са посочени в Таблица 1.

| **Искане на субекта на данни** | **Срок** |
|---|---|
| Правото да бъде информиран | Когато данните са събрани (ако са предоставени от субекта на данни) или в рамките на един месец (ако не са предоставени от субекта на данни) |
| Правото на достъп | Един месец |
| Правото на коригиране | Един месец |
| Правото за изтриване | Без неоправдано забавяне |
| Правото да се ограничи обработката | Без неоправдано забавяне |
| Правото на преносимост на данни | Един месец |
| Право на възражение | При получаване на възражение |
| Права във връзка с автоматизираното вземане на решения и профилиране - неприложимо. | Неприложимо |

**7.Законосъобразност на обработване**

Съществуват шест алтернативни начина, по които законосъобразността на конкретен случай на обработка на лични данни може да бъде установена в рамките на GDPR. Политиката на РЗИ-Кюстендил е да идентифицира подходящата база за обработка и да я документира в съответствие с регламента.

**8.Съгласие**

Освен ако не е необходимо поради причина, допустима в GDPR, РЗИ-Кюстендил винаги ще поиска изрично съгласие от субекта на данни да събира и обработва данните му. В случай на деца под 18-годишна възраст или поставени под запрещение лица, ще бъде поискано съгласието на родител/настойник/попечител. Субектите могат да упражнят правата си съгласно GDPR (искане за достъп до личните си данни, коригиране, ограничаване на обработването, отказ от автоматично профилиране, заличаване) по ред установен и комуникиран с тях, в рамките на закона, безплатно и в срок до 30 дни, след подаване на искането.

**9.Изпълнение на договор**

Когато личните данни, събрани и обработени са необходими за изпълнение на договор със субекта на данните, не се изисква изрично съгласие. Това често се случва, когато договорът не може да бъде завършен и изпълнен без въпросните лични данни.

**10.Правно задължение**

Ако се изисква да се събират и обработват личните данни, за да се спази законът, не се изисква изрично съгласие. Това може да е случаят с някои данни, свързани с трудови и служебни взаимоотношения, социално осигуряване, данъчното облагане, административнонаказателна дейност.

**11.Жизненоважни интереси на субекта на данни**

В случаите, когато личните данни са необходими за защита на жизненоважните интереси на субекта на данните или на друго физическо лице, това може да се използва като законова основа на обработката и РЗИ-Кюстендил ще запази разумни и документирани доказателства, че случаят е такъв, когато тази причина се използва като законова основа за обработката на лични данни. Това се прилага например при случаи от обществена значимост.

**12.Изпълнение на задача от обществен интерес**

Когато Инспекцията трябва да изпълни задача, която смята, че е в обществен интерес или като част от служебно задължение, тогава съгласието на субекта на данните няма да бъде поискано. Оценката на обществения интерес или на служебното задължение ще бъде документирана и предоставена като доказателство при необходимост.

**13.Законови интереси**

Ако обработването на конкретни лични данни е в законовите интереси на РЗИ-Кюстендил и се счита, че това не засяга съществено правата и свободите на субекта на данните, това може да се определи като законово основание за обработката. Отново, аргументите зад този възглед ще бъдат документирани.

**14.Защита на правото на поверителност**

РЗИ-Кюстендил е приел/а принципа на поверителност при проектиране (нововъведения) и ще гарантира, че определянето и планирането на всички нови или значителни промени в процесите, при които се събират или обработват лични данни, ще бъдат обект на надлежно отчитане на въпросите, свързани с поверителността, включително завършването на една или повече оценки на въздействието върху защитата на данните.

Оценката на въздействието върху защита на данните ще включва:

- да се вземе предвид как ще се обработват личните данни и за какви цели;
- оценка дали предложената обработка на лични данни е необходима и пропорционална на целта (целите);
- оценка на рисковете за физическите лица при обработката на личните данни
- Какви контролни механизми са необходими за справяне с установените рискове и за доказване на спазването на законодателството

**15.Длъжностно лице по защита на данни**

Съгласно GDPR, ако дадена организация е публичен орган, ако извършва мащабен мониторинг или обработва особено чувствителни типове данни в голям мащаб, се изисква определена роля на Длъжностно лице по защита на данните (ДЛЗД). ДЛЗД се изисква да притежава подходящо ниво на знания и може да бъде или вътрешен ресурс, или да се възложи на външен подходящ доставчик на услуги. На базата на тези критерии, РЗИ-Кюстендил има Длъжностно лице по защита на данните.

**16.Уведомление за нарушение**

Политиката на РЗИ-Кюстендил прилага принципите за справедливост и пропорционалност, когато разглежда действията, които трябва да се предприемат, за да се информират засегнатите страни относно нарушения на лични данни. В съответствие с GDPR, за всяко установено нарушение на сигурноста на личните данни – умишлено изтичане на лични данни; неправомерно предоставяне на трети стани или изтриване, случайно унищожаване или загуба; увреждане целостта на данните и всяко друго действие, което е вероятно да доведе до риск за правата и свободите на субектите на данни, Длъжностното лице по защита на лични данни при РЗИ - Кюстендил информира незабавно Комисията по защита на лични данни при установено нарушение, не по-късно от 72 часа, след като е узнало за него, освен ако длъжностното лице не е в състояние да докаже в съответствие с принципа за отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите

лица. При нарушаване на правата му, субектът на данни разполага със средствата за правна защита и може да търси отговорност за причинените му вреди.

**17.Уведомяване на субекта на данни**

Когато лични данни се събират от субекта на данни, в момента на събирането им, РЗИ-Кюстендил уведомява лицата по ясен и непротиворечив начин каква информация за тях ще бъде обработена, разкрита и съхранявана, за какви цели, и правата им по отношение на защитата на личните данни. Това уведомяване е съобразено с изискванията на Регламента и цели спазването му, включително, но не само, принципа за прозрачност и законосъобразност при обработката на личните данни на лицата.

**18.Как се обработват лични данни**

РЗИ-Кюстендил гарантира, че се обработват само лични данни, които са необходими за всяка конкретна цел. Взети са мерки за защита на личните данни от случайна загуба и нерегламентиран достъп, употреба, промяна или оповестяване. Освен това са взети допълнителни мерки за информационна сигурност, включително контрол на достъпа, строга физическа защита и надеждни практики за събиране, съхранение и обработка на информацията. Въведени са технически и организационни мерки, ограничаващи нерегламентирания достъп, копиране, промяна и заличаване на лични данни. По отношение на личните данни, съхранявани на електронен носител, достъпът до компютърните устройства, съхраняващи данните, се осъществява само от оторизираните за това лица.

**19.Срок на обработка**

РЗИ- Кюстендил съхранява данни в минимален обем и за срок не по-дълъг от необходимия за всяка категория данни, определени от нормативната уредба на страната. Заличаване на лични данни се извършва само след отпадане основанието за обработка и съхранение, и след преценка на специалните законови изисквания. В случай, че за някои лични данни е предвиден законов срок за съхраняването им, не се допуска унищожаване на тези лични данни преди изтичането му. Не се допуска и унищожаване на лични данни при наличие на легитимен интерес или необходими за упражняване на права и задължения на администратора. Унищожаването на данни се извършва съгласно процедури, одобрени от администратора.

**20.С кого се споделят лични данни**

Лични данни могат да бъдат предоставени на:

- публични органи (МЗ, НОИ, НАП, МВР, съдилища, прокуратура, и други), по силата на действащото законодателство;
- обработващ лични данни – физически или юридически лица, които обработват лични данни на РЗИ, възложени чрез договор (само за служители);
- при използване на куриерски услуги – приемане и доставка, адресиране на пратки до физически лица (имена и адрес);

- работодатели - за целите на медицинската експертиза.

**21.Ред за упражняване на правата на субекта на данни**

Действията по упражняване правата на субекта на данните се извършват лично от лицето или от пълномощник с изрично пълномощно, с нотариална заверка на подписа, на адреса на управление на администратора, **чрез писмено заявление**.

РЗИ-Кюстендил съдейства за упражняването на правата на субекта на данните, като му предоставя информация относно действията, предприети във връзка с искане по упражняване на правата на субекта на данните. Информацията, предоставяна на субекта, и всяка комуникация и действия по упражняване правата на субекта на данни се предоставят безплатно. Когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искане за упражняване на правата, администраторът може да поиска предоставянето на допълнителна информация, необходима за потвърждаване самоличността на субекта на данните.

**22.Трансфер на лични данни**

Обработката, съхранението и трансферът на лични данни е обезпечен със съвременни технически средства. Администраторът няма да прехвърлят събираните и обработваните лични данни извън рамките на Европейското икономическо пространство без спазване на законовите възможности, като ще въведат всички подходящи предпазни мерки, с цел спазване на поверителност информацията.

**23.Сигурност на личните данни**

РЗИ-Кюстендил прилага подходящи технически и организационни мерки за осигуряване нивото на сигурност, съобразено с рисковете с различна вероятност и тежест и правата и свободите на физическите лица, за което е въвел следните мерки:

- на служителите с достъп до лични данни е проведено обучение. Същите са поели ангажимент за поверителност;
- контрол на физическия и логически достъп до хартиени и електронни регистри с лични данни;
- контрол при използването на преносими електронни устройства извън работното място;
- налагане на договорни задължения на обработващите лични данни организации, за педприемане на подходящи мерки за сигурност, когато данните са под техен контрол;

**24.Адресиране на съответствието с GDPR**

Следните действия са предприети, за да се осигури, че РЗИ-Кюстендил отговаря по всяко време на принципа за отчетност на GDPR:

- правната основа за обработването на лични данни е ясна и недвусмислена;
- налично е Длъжностно лице по защита на данните със специална отговорност за защитата на данните в организацията;

- целият персонал, ангажиран с обработването на лични данни, разбира своите отговорности за спазването на добрите практики за защита на данните;
- обучението по защита на данните е предоставено на целия персонал;
- правилата за съгласие се спазват;
- субектите на данни могат да упражнят своите права по отношение на личните данни и запитванията им се обработват ефективно;
- провеждат се редовни прегледи на процедурите, регламентиращи обработката на лични данни;
- поверителността се прилага за всички нововъведения в процесите и дейностите;
- записва се следната информация за обработващите дейности:
    -име на организацията и съответните детайли
    -цел на обработката на лични данни
    -категории лица и обработени лични данни
    -категории получатели на лични данни
    -срокове за запазване на личните данни
    -съществуващ технически и организационен контрол

Тези действия се преглеждат редовно като част от процеса на управление, свързан със защитата на данните.

РЗИ-Кюстендил запазва правото си да изменя и допълва настоящата Политика в съответствие с настъпилите промени в приложимото законодателство и в развитието на технологиите за защита.

Изготвил:

**Райничка Стоянова**

Главен секретар на РЗИ - Кюстендил