



ПРИКАЗ

26.08.2015

БОЕРЫК

№ 1715

г. Казань

Об утверждении Политики безопасности  
персональных данных

Во исполнение Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», п р и к а з ы в а ю :

1. Утвердить Политику безопасности персональных данных (приложение).
2. Начальнику отдела информационных и инновационных технологий М.С. Нурмиеву обеспечить размещение Политики безопасности персональных данных на официальном сайте Министерства здравоохранения Республики Татарстан в десятидневный срок со дня утверждения.
3. Начальнику отдела кадров А.Ф. Салаватовой обеспечить ознакомление с Политикой безопасности персональных данных, утвержденной пунктом 1 настоящего приказа, лиц, принимаемых на работу, до подписания служебного контракта (трудового договора), под личную подпись.
4. Руководителям структурных подразделений Министерства здравоохранения Республики Татарстан ознакомить с Политикой безопасности персональных данных, утвержденной пунктом 1 настоящего приказа, сотрудников Министерства.
5. Контроль исполнения настоящего приказа возложить на заместителя министра здравоохранения Республики Татарстан И.Р. Фатихова.

Министр

А.Ю. Вафин



## ПОЛИТИКА безопасности персональных данных

### Термины и определения

В настоящей Политике безопасности персональных данных в Министерстве здравоохранения Республики Татарстан (далее – Министерство), устанавливающей процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, используются следующие термины и определения:

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

**Оператор** – (Министерство здравоохранения Республики Татарстан) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

**Автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

**Предоставление персональных данных** – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

**Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в



информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

**Информационная система персональных данных** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

**Несанкционированный доступ к информации** – неправомерное получение, использование, утрата, уничтожение, искажение, блокирование информации;

**Допуск к информации** – официальное разрешение субъекту обращаться к информации определенного уровня конфиденциальности.

### Перечень сокращений

АРМ	Автоматизированное рабочее место
ПДн	Персональные данные
СЗИ	Средства защиты информации
СЗПДн	Система защиты персональных данных
ИС	Информационная система
ИСПДн	Информационная система персональных данных

## 1. Общие положения

1.1. Настоящая Политика безопасности персональных данных (далее – Политика) определяет порядок обработки и защиты персональных данных в Министерстве здравоохранения Республики Татарстан (Министерство).

1.2. Основанием для разработки данного локального нормативного акта являются:

Конституция Российской Федерации;

Гражданский кодекс Российской Федерации;

Трудовой кодекс Российской Федерации;

Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;

Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;



Федеральный закон от 29.11.2010 № 326-ФЗ «О медицинском страховании в Российской Федерации»;

Постановление Правительства Российской Федерации от 22.12.2011 № 1081 «О лицензировании фармацевтической деятельности»;

Постановление Правительства Российской Федерации от 16.04.2012 № 291 «О лицензировании медицинской деятельности»;

Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

Постановление Кабинета Министров Республики Татарстан от 22.02.2013 № 128 «О внесении изменений в отдельные постановления Кабинета Министров Республики Татарстан».

1.3. Персональные данные относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере негосударственной (служебной, профессиональной) тайны.

## **2. Цели сбора обработки и хранения персональных данных**

Целью сбора, обработки и хранения персональных данных субъектов персональных данных является:

1. Организации кадрового учета Министерства, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по служебным контрактам, трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, другими федеральными законами;

2. Регистрация сведений, необходимых для реализации полномочий государственного органа в сфере здравоохранения: по вопросам организации медицинской профилактики, в том числе инфекционных заболеваний и СПИД, медицинской помощи и медицинской реабилитации, лекарственного обеспечения, деятельности, связанной с оборотом наркотических средств, психотропных веществ и их прекурсоров;



3. Рассмотрение обращений граждан в пределах компетенции Министерства.

### **3. Перечень персональных данных, обрабатываемых в Министерстве**

3.1. Министерство обрабатывает следующие персональные данные государственных гражданских служащих и работников Министерства (далее – сотрудников):

Фамилия, имя, отчество (в т.ч. прежние), дата и место рождения;

Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство;

Национальность;

Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания;

Сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки (серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками и другие сведения);

Сведения о повышении квалификации и переподготовке (серия, номер, дата выдачи документа о повышении квалификации или о переподготовке, наименование и местоположение образовательного учреждения, дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения и другие сведения);

Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, наименования, адреса и служебного телефона, а также реквизитов других организаций с полным наименованием занимаемых ранее в них должностей и времени работы в этих организациях, а также другие сведения) сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);

Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней;

Содержание и реквизиты служебного контракта, трудового договора с работником Министерства, или гражданско-правового договора с гражданином;

Сведения о заработной плате (номера счетов для расчета с работниками, данные схем вознаграждения с клиентами или партнерами, в том числе номера их спецкартсчетов);

Сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет, военно-учетная специальность, воинское звание, данные о принятии/снятии на(с) учет(а) и другие сведения);



Сведения о семейном положении (состояние в браке, данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта (при наличии), данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам (при наличии), степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев и другие сведения, в т.ч. социальное положение);

Сведения об имуществе сотрудников (имущественном положении, включая транспорт, недвижимость, кредиты или займы);

Сведения о номере и серии страхового свидетельства государственного пенсионного страхования;

Сведения об идентификационном номере налогоплательщика;

Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования);

Сведения, указанные в оригиналах и копиях приказов по сотрудникам Министерства и материалах к ним;

Сведения о государственных и ведомственных наградах, почетных и специальных званиях, поощрениях (в том числе наименование или название награды, звания или поощрения, дата и вид нормативного акта о награждении или дата поощрения) сотрудников Министерства;

Материалы по аттестации и отзывы о профессиональном уровне сотрудников;

Материалы по внутренним служебным расследованиям;

Медицинские заключения о состоянии здоровья, сведения о временной нетрудоспособности;

Табельный номер;

Номера телефонов (мобильного и домашнего);

Сведения о социальных льготах и о социальном статусе (серия, номер, дата выдачи, наименование органа, выдавшего документ, являющийся основанием для предоставления льгот и статуса, и другие сведения);

Сведения для получения информации о возможных фактах осуждения к наказанию, исключающему возможность исполнения должностных обязанностей по должности государственной службы, по приговору суда, вступившему в законную силу через Информационный центр МВД по РТ.

3.2. Министерство обрабатывает следующие категории персональных данных граждан, не являющихся сотрудниками Министерства (субъекты):

Фамилия, имя, отчество;

Дата и место рождения;

Адрес места жительства (по паспорту и фактический);

Контактный номер телефона;

Электронный адрес;

Национальность (только наградные материалы);

Сведения об образовании;

Место работы;

Должность;

Стаж;



Социальное положение;  
Паспортные данные;  
Сведения о научных трудах;  
Знание иностранного языка;  
Сведения, содержащиеся в полисе медицинского страхования;  
Сведения, содержащиеся в свидетельстве о рождении;  
Сведения о состоянии здоровья (в том числе группа здоровья, группа инвалидности), заболеваниях, результаты выполненных медицинских исследований;  
Сведения, содержащиеся в страховом свидетельстве государственного пенсионного страхования (СНИЛС).

#### **4. Принципы обработки персональных данных**

При организации технологического процесса обработки персональных данных в Министерстве сотрудники, допущенные к обработке ПДн, должны руководствоваться следующими основными принципами:

- соблюдение законности целей и способов обработки ПДн;
- контроль достоверности ПДн и их достаточности для достижения заявленной цели;
- соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн;
- недопустимость обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- соответствие объема, содержания и характера обрабатываемых ПДн, способа обработки ПДн целям обработки ПДн;
- соблюдение условий конфиденциальности ПДн в пределах взятых на себя обязательств, в соответствии с действующим законодательством Российской Федерации;
- исключение возможности обработки одного и того же массива ПДн в прикладных информационных системах (в том числе автоматизированных системах), различающихся по целевому назначению;
- обработка, хранение ПДн должны осуществляться в форме, позволяющей определить субъект ПДн, не дольше, чем этого требуют цели их обработки; по достижении цели обработки либо утраты необходимости в обработке ПДн подлежат уничтожению;
- обеспечение защиты информации.

#### **5. Порядок предоставления допуска и доступа к персональным данным**

К работе с персональными данными, обрабатываемыми в Министерстве, допускаются сотрудники в соответствии с утверждаемыми Списками должностей работников, уполномоченных на автоматизированную и неавтоматизированную обработку ПДн.



Допуск к работе с персональными данными оформляется после ознакомления сотрудника с должностной инструкцией (должностными обязанностями), с положениями Политики и подписания обязательства о неразглашении персональных данных, обрабатываемых в Министерстве.

Все лица, получившие доступ к персональным данным, обрабатываемым в Министерстве, обязаны не распространять их и не раскрывать их третьим лицам.

## **6. Порядок получения персональных данных**

6.1. Получение персональных данных преимущественно осуществляется путем представления их самим гражданином, на основании его письменного согласия, за исключением случаев прямо предусмотренных действующим законодательством.

В случаях, предусмотренных федеральным законодательством, обработка персональных данных осуществляется только с согласия гражданина в письменной форме. Равнозначным содержащему собственноручную подпись гражданина согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законодательством электронной подписью. Согласие гражданина в письменной форме на обработку его персональных данных должно включать в себя, в частности:

фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

наименование или фамилию, имя, отчество и адрес Министерства, получающего согласие субъекта персональных данных;

цель обработки персональных данных;

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Министерства, если обработка будет поручена такому лицу;

перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Министерством-оператором способов обработки персональных данных;

срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законодательством;

подпись субъекта персональных данных.



Для обработки персональных данных, содержащихся в согласии в письменной форме гражданина на обработку его персональных данных, дополнительное согласие не требуется.

В случае недееспособности гражданина или недостижения гражданином 15 лет согласие на обработку его персональных данных дает в письменной форме его законный представитель.

## **7. Порядок хранения и использования персональных данных**

7.1. Персональные данные в Министерстве обрабатываются с соблюдением требований действующего законодательства Российской Федерации о защите персональных данных.

7.2. В Министерстве используется смешанная обработка персональных данных: неавтоматизированная и автоматизированная.

7.3. Порядок хранения персональных данных в Министерстве должно исключать возможность утраты ПДн и/или их неправомерное использование.

7.4. Сроки обработки и хранения ПДн в Министерстве определяются: достижением цели обработки ПДн; сроком исковой давности, а также иными требованиями законодательства Российской Федерации в части осуществления архивного хранения документов, образующихся в результате деятельности государственных органов, органов местного самоуправления и организаций.

Ответственные лица за хранение документов, содержащих персональные данные, назначаются приказом министра здравоохранения Республики Татарстан.

7.5. Хранение окончанных производством документов, содержащих персональные данные, осуществляется в помещениях Министерства, предназначенных для хранения отработанной документации.

Ответственные лица за хранение окончанных производством документов, содержащих персональные данные, назначаются приказом министра здравоохранения Республики Татарстан.

7.6. Материальные носители, содержащие персональные данные, журналы учета материальных носителей должны храниться в сейфах, запирающихся шкафах либо специально выделенных для хранения помещениях с регламентированным доступом.

## **8. Порядок уничтожения персональных данных**

Уничтожение ПДн с носителей ПДн или же самих носителей, содержащих ПДн, производится:

по достижении целей обработки согласно номенклатуре дел и документов;  
по достижении окончания срока хранения ПДн, оговоренного в соответствующем соглашении заинтересованных сторон, в том числе, если они не подлежат архивному хранению.

Уничтожение персональных данных производится в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти



рабочих дней с момента выявления неправомерной обработки персональных данных.

Уничтожение информации с ПДн, хранящейся в электронном виде на материальных носителях, производится путем выполнения процедуры специальной подготовки материальных носителей (многократное форматирование разделов, выделенных под хранение данных).

Уничтожение материальных носителей с ПДн осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.).

Уничтожение производится по мере необходимости, в зависимости от накопленных объемов.

Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2 человек. Уничтожение осуществляется по акту.

Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, иные носители, содержащие ПДн, подлежащие уничтожению, должны храниться отдельно.

## **9. Порядок передачи персональных данных**

9.1. При передаче персональных данных субъекта сотрудникам Министерства должны соблюдаться следующие требования:

предупредить лиц, получающих персональные данные субъекта ПДн, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности;

разрешать доступ к персональным данным только специально уполномоченным лицам, определенным приказом по Министерству, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций.

9.2. Передача персональных данных третьим лицам осуществляется Министерством только с письменного согласия субъекта, в случаях, прямо предусмотренных федеральными законами. Лица, которым в установленном Федеральным законом «О персональных данных» порядке переданы сведения, составляющие персональные данные субъекта, несут дисциплинарную, административную или уголовную ответственность за разглашение в соответствии с законодательством Российской Федерации.

9.3. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законодательством на получение персональных данных субъекта, либо отсутствует письменное согласие субъекта на передачу его персональных данных, Министерство обязано отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдается мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится у Министерства.



9.4. Транспортировка, передача носителей персональных данных должна происходить в порядке, исключающем случайную утрату носителей или утечку персональных данных.

## 10. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы, создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Министерства.

10.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных, либо персонал, имеющий право доступа в помещения, в которых обрабатываются ПДн. Регламентация доступа персонала к документам и базам данных с персональными данными входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий прав доступа пользователей к персонифицированной информации. Для защиты персональных данных субъектов необходимо соблюдать ряд мер:

ограничение и регламентация состава сотрудников Министерства, функциональные обязанности которых требуют доступа к ПДн;

строгое избирательное и обоснованное распределение документов и информации между сотрудниками Министерства;

рациональное размещение рабочих мест сотрудников Министерства, при котором исключалось бы бесконтрольное использование и просмотр защищаемой информации;

знание сотрудниками Министерства требований нормативных методических документов по защите информации и сохранении тайны;

наличие необходимых условий в помещении для работы с документами и базами данных с персональными сведениями;

определение и регламентация состава сотрудников Министерства, имеющих право доступа (входа) в помещения, в которых обрабатываются персональные данные;

организация порядка уничтожения информации;



своевременное выявление нарушений требований разрешительной системы доступа сотрудникам подразделения;

воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с документами, содержащими персональные данные;

не допускается вынос личных дел сотрудников Министерства за пределы помещения, в котором они хранятся.

10.2. Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Министерства, посетители, работники других организаций и ведомств.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Министерстве.

10.2.1. Для защиты персональных данных необходимо соблюдать ряд мер:

порядок приема, учета и контроля деятельности посетителей;

пропускной режим в Министерстве;

технические средства охраны, сигнализации;

порядок охраны территории, зданий, помещений, транспортных средств;

требования к защите информации при интервьюировании и беседах.

10.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

## **11. Права субъекта персональных данных**

11.1. В целях обеспечения защиты персональных данных, обрабатываемых в Министерстве, субъект персональных данных имеет право:

получать полную информацию о своих персональных данных и их обработке;

свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных федеральным законодательством. Получение указанной информации о своих персональных данных возможно при личном обращении в Министерство;

требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Федерального закона «О персональных данных». Указанное требование должно быть оформлено



письменным заявлением субъекта персональных данных на имя министра здравоохранения Республики Татарстан;

обжаловать в суде любые неправомерные действия или бездействия должностных лиц Министерства при обработке и защите персональных данных.

## **12. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных**

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

12.1. Руководители Управлений и отделов Министерства, разрешающие в нарушение установленных правил доступ к конфиденциальному документу, несет в этой связи персональную ответственность.

12.2. Каждый государственный служащий и работник Министерства, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность информации.

12.3. Лица, виновные в нарушении норм, регулирующих получение, обработку, хранение и передачу персональных данных субъектов персональных данных, несут ответственность, предусмотренную действующим законодательством.

## **13. Право на обжалование действий или бездействия Министерства**

13.1. Если субъект персональных данных, его законный представитель или сотрудник Министерства считает, что Министерство осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Министерства в уполномоченный орган по защите прав субъектов персональных данных (Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи) или в судебном порядке.

13.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

13.3. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.



## 14. Заключительные положения

14.1. Настоящая Политика вступает в силу с даты её утверждения.

14.2. При необходимости приведения настоящей Политики в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании приказа министра здравоохранения Республики Татарстан.

14.3. Настоящая Политика распространяется на всех сотрудников Министерства, имеющих доступ и осуществляющих обработку персональных данных сотрудников Министерства и субъектов персональных данных, не являющихся сотрудниками Министерства.

14.4. Субъекты персональных данных, не являющиеся сотрудниками Министерства, а так же их законные представители имеют право ознакомиться с настоящей Политикой.

14.5. Сотрудники Министерства здравоохранения Республики Татарстан подлежат ознакомлению с данным документом в порядке, предусмотренном приказом министра здравоохранения Республики Татарстан, под личную подпись.

14.6. В обязанности государственных гражданских служащих, осуществляющих первичный сбор персональных данных физического лица, входит получение согласия физического лица на обработку его персональных данных под личную подпись.

14.7. В обязанности представителя нанимателя входит ознакомление всех сотрудников Министерства с настоящей Политикой и лиц, принимаемых на работу до подписания служебного контракта (трудового договора), под личную подпись.

14.8. Документы, определяющие политику в отношении обработки персональных данных сотрудников Министерства, должны быть размещены на официальном сайте или информационном стенде Министерства в десятидневный срок после их утверждения.