

**Государственное бюджетное учреждение здравоохранения «Армавирский
кожно-венерологический диспансер» министерства здравоохранения
Краснодарского края**

ПРИКАЗ

от 25.06.2024

№ 305-17

г. Армавир

**О мерах, направленных на обеспечение выполнения
обязанностей, предусмотренных Федеральным законом от
27 июля 2006 г. № 152-ФЗ «О персональных данных» и
принятыми в соответствии с ним нормативными правовыми
актами**

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и принятыми в соответствии с ним нормативными правовыми актами, п р и к а з ы в а ю:

1. Утвердить:

1) Правила обработки персональных данных субъектов персональных данных в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 1);

2) Правила рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 2);

3) Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 3);

4) Перечень информационных систем персональных данных государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 4);

5) Инструкцию пользователя, допущенного к обработке персональных данных в информационных системах государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 5);

6) Типовое обязательство сотрудника государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора прекратить обработку персональных данных, ставших известными ему, в связи с исполнением должностных обязанностей (приложение 6);

7) Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение 7);

8) Порядок доступа сотрудников государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края в помещения, в которых ведётся обработка персональных данных (приложение 8);

9) Положение по работе с инцидентами информационной безопасности в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 9);

10) Инструкцию по учёту, хранению и регистрации выдачи машинных носителей персональных данных государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (приложение 10);

11) Форму журнала ознакомления сотрудников государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) обучения указанных сотрудников (приложение 11).

2. Контроль за выполнением настоящего приказа оставляю за собой.

3. Приказ вступает в силу со дня его подписания.

И.о. главного врача

С.А. Фурсенко



Приложение 1

УТВЕРЖДЕНЫ

приказом ГБУЗ Армавирского КВД

от 25.06.2024 № 305-17

ПРАВИЛА
обработки персональных данных субъектов персональных
данных в государственном бюджетном учреждении
здравоохранения «Армавирский кожно-венерологический
диспансер» министерства здравоохранения Краснодарского
края

1. Основные понятия

В настоящем документе используются следующие основные понятия:

автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных — состояние защищённости персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий, и технических средств;

конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

несанкционированный доступ (несанкционированные действия) — доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам;

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;

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

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

персональные данные – любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу (субъекту персональных данных);

персональные данные, разрешённые субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путём дачи согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации),

программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

2. Общие положения

Настоящие правила обработки персональных данных субъектов персональных данных (далее – Правила) разработаны для обеспечения безопасности персональных данных, а также защиты прав и свобод граждан при их обработке, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным (далее также – ПДн) субъектов, за невыполнение требований норм и правил, регулирующих обработку и защиту ПДн в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение).

Настоящие Правила устанавливают порядок обработки ПДн субъектов в Бюджетном учреждении и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере ПДн.

Субъектами ПДн в Бюджетном учреждении являются:

- 1) ближайшие родственники сотрудника;
- 2) клиенты;
- 3) клиенты (платные пациенты);
- 4) контрагенты;

- 5) сотрудники;
- 6) уволенные (уволившиеся) сотрудники и их ближайшие родственники;
- 7) члены профсоюза.

Под обработкой ПДн понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Настоящие Правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к ПДн. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты ПДн.

Настоящие Правила разработаны в соответствии со следующими нормативно-правовыми актами (документами) Российской Федерации:

- 1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 г., ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;
- 2) Конституция Российской Федерации;
- 3) Гражданский кодекс Российской Федерации;
- 4) Кодекс Российской Федерации об административных правонарушениях;
- 5) Трудовой кодекс Российской Федерации;
- 6) Уголовный кодекс Российской Федерации;
- 7) Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- 8) Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 9) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 г. № 188;
- 10) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое

постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;

11) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

В соответствии с законодательством Российской Федерации об обработке и защите ПДн, ПДн субъектов являются конфиденциальной информацией.

Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн. Обработке подлежат только те ПДн, которые отвечают целям их обработки и не должны быть избыточными по отношению к заявленным целям.

При обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн.

Деятельность по организации обработки и защиты ПДн, в соответствии с требованиями законодательства Российской Федерации о ПДн, осуществляет сотрудник Бюджетного учреждения, назначенный ответственным за организацию обработки ПДн в Бюджетном учреждении.

Деятельность по администрированию средств и механизмов защиты осуществляет сотрудник Бюджетного учреждения, назначенный администратором информационной безопасности в Бюджетном учреждении.

Техническое обслуживание информационных систем ПДн осуществляет сотрудник Бюджетного учреждения, назначенный ответственным за техническое обслуживание информационных систем ПДн в Бюджетном учреждении.

Ответственный за организацию обработки ПДн, администратор информационной безопасности и ответственный за техническое обслуживание информационных систем ПДн назначаются приказом и.о. главного врача.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования, уничтожения документов и других материальных носителей ПДн определяет законодательство Российской Федерации об обработке и защите ПДн, а также действующие нормативные правовые акты Бюджетного учреждения.

Бюджетное учреждение является оператором ПДн субъектов, указанные в настоящих Правилах. Бюджетное учреждение вправе поручить обработку ПДн третьим лицам с согласия субъекта ПДн, если иное не предусмотрено

федеральным законом, на основании заключаемого с этим лицом соглашения (договора), либо путём принятия соответствующего акта (далее – поручение Бюджетного учреждения). Лицо, осуществляющее обработку ПДн по поручению Бюджетного учреждения, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Федеральным законом № 152-ФЗ. В поручении Бюджетного учреждения должны быть определены перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку ПДн, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПДн, требования, предусмотренные частью 5 статьи 18 и статьёй 18.1 Федерального закона № 152-ФЗ, обязанность по запросу Бюджетного учреждения в течение срока действия поручения Бюджетного учреждения, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Бюджетного учреждения требований, установленных в соответствии с Федеральным законом № 152-ФЗ, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьёй 19 Федерального закона № 152-ФЗ, в том числе требование об уведомлении Бюджетного учреждения о случаях, предусмотренных частью 3.1 статьи 21 Федерального закона № 152-ФЗ.

Лицо, осуществляющее обработку ПДн по поручению Бюджетного учреждения, не обязано получать согласие субъекта ПДн на обработку его ПДн.

В случаях, когда Бюджетное учреждение поручает обработку ПДн третьему лицу, ответственность перед субъектом ПДн за действия указанного лица несёт Бюджетное учреждение. Лицо, осуществляющее обработку ПДн по поручению Бюджетного учреждения, несёт ответственность перед Бюджетным учреждением.

В случае, если Бюджетное учреждение поручает обработку ПДн иностранному физическому лицу или иностранному юридическому лицу, ответственность перед субъектом ПДн за действия указанных лиц несёт Бюджетное учреждение и лицо, осуществляющее обработку ПДн по поручению Бюджетного учреждения.

Бюджетное учреждение и иные лица, получившие доступ к ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом.

Рекомендуемая типовая форма поручения (соглашения (договора)) обработки ПДн приведена в приложении 1 к Правилам. Типовую форму поручения обработки ПДн необходимо использовать при заключении договоров

(контрактов) и дополнительных соглашений с контрагентами, по которым предполагается передача контрагенту ПДн субъектов.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, Бюджетное учреждение вправе получать и обрабатывать данные о частной жизни сотрудников Бюджетного учреждения только с их письменного согласия.

В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги). В общедоступные источники ПДн с письменного согласия субъекта ПДн могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн, сообщаемые субъектом ПДн.

Сведения о субъекте ПДн должны быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

Бюджетное учреждение не имеет права получать и обрабатывать ПДн субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами.

Все изменения в Правила вносятся приказом и.о. главного врача.

3. Цель и содержание обработки персональных данных

Целями обработки ПДн в Бюджетном учреждении являются:

- 1) ведение бухгалтерского учета;
- 2) исполнение договора с субъектом;
- 3) обработка в соответствии с трудовым законодательством;
- 4) оказание медицинских услуг (помощи) населению, в том числе платных и иных услуг, в соответствии с уставом.

Цель «ведение бухгалтерского учета» достигается посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

- 1) контрагенты:

Иные категории ПДн: адрес, адрес электронной почты, год рождения, гражданство, дата рождения, доходы, занимаемая должность, ИНН, контактные сведения, место рождения, паспортные данные, реквизиты лицевого/расчетного счета, судимость, сумма контракта/договора, фамилия, имя, отчество.

2) сотрудники:

Иные категории ПДн: адрес, адрес электронной почты, год рождения, гражданство, данные водительского удостоверения, данные полиса омс, дата рождения, доходы, занимаемая должность, имущественное положение, ИНН, информация о трудовой деятельности, контактные сведения, место рождения, национальная принадлежность, образование, паспортные данные, профессия, реквизиты лицевого/расчетного счета, сведения о воинском учёте, сведения о наградах, семейное положение, СНИЛС, состав семьи, социальное положение, степень родства, судимость, трудоспособность, фамилия, имя, отчество, фотография.

Способ обработки персональных данных: смешанный тип обработки персональных данных со следующими действиями с персональными данными: блокирование; запись; извлечение; использование; накопление; обезличивание; сбор; систематизация; удаление; уничтожение; уточнение (обновление, изменение); хранение.

Срок обработки ПДн: 50 лет, срок хранения ПДн: 50 лет.

Цель «исполнение договора с субъектом» достигается посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) клиенты (платные пациенты):

Иные категории ПДн: адрес, контактные сведения, паспортные данные, фамилия, имя, отчество.

Способ обработки персональных данных: смешанный тип обработки персональных данных со следующими действиями с персональными данными: запись; извлечение; использование; накопление; сбор; систематизация; удаление; уничтожение; уточнение (обновление, изменение); хранение.

Срок обработки ПДн: 50 лет, срок хранения ПДн: 50 лет.

Цель «обработка в соответствии с трудовым законодательством» достигается посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) ближайшие родственники сотрудника:

Специальные категории ПДн: национальная принадлежность, судимость.

Иные категории ПДн: адрес, год рождения, гражданство, данные водительского удостоверения, данные полиса омс, дата рождения, доходы, занимаемая должность, ИНН, информация о трудовой деятельности, контактные сведения, место рождения, национальная принадлежность, образование, паспортные данные, профессия, реквизиты лицевого/расчетного счета, сведения о воинском учёте, сведения о наградах, семейное положение, СНИЛС, состав

семьи, социальное положение, степень родства, трудоспособность, фамилия, имя, отчество.

2) уволенные (уволившиеся) сотрудники и их ближайшие родственники:

Иные категории ПДн: адрес, год рождения, гражданство, данные водительского удостоверения, данные полиса омс, дата рождения, доходы, занимаемая должность, имущественное положение, ИНН, информация о трудовой деятельности, контактные сведения, место рождения, национальная принадлежность, образование, паспортные данные, профессия, реквизиты лицевого/расчетного счета, сведения о воинском учёте, сведения о наградах, семейное положение, СНИЛС, состав семьи, социальное положение, степень родства, судимость, трудоспособность, фамилия, имя, отчество, фотография.

3) члены профсоюза:

Иные категории ПДн: адрес, год рождения, дата рождения, занимаемая должность, контактные сведения, образование, профессия, фамилия, имя, отчество, фотография.

Способ обработки персональных данных: смешанный тип обработки персональных данных со следующими действиями с персональными данными: запись; извлечение; использование; накопление; сбор; систематизация; удаление; уничтожение; уточнение (обновление, изменение); хранение.

Срок обработки ПДн: 50 лет, срок хранения ПДн: 50 лет.

Цель «оказание медицинских услуг (помощи) населению, в том числе платных и иных услуг, в соответствии с уставом» достигается посредством обработки ПДн следующих категорий для следующих субъектов ПДн:

1) Клиенты:

Иные категории ПДн: данные полиса омс, дата рождения, паспортные данные, пол, СНИЛС, фамилия, имя, отчество.

2) клиенты (платные пациенты):

Иные категории ПДн: адрес, контактные сведения, паспортные данные, фамилия, имя, отчество.

3) уволенные (уволившиеся) сотрудники и их ближайшие родственники:

Иные категории ПДн: адрес, год рождения, гражданство, данные водительского удостоверения, данные полиса омс, дата рождения, доходы, занимаемая должность, имущественное положение, ИНН, информация о трудовой деятельности, контактные сведения, место рождения, национальная принадлежность, образование, паспортные данные, профессия, реквизиты лицевого/расчетного счета, сведения о воинском учёте, сведения о наградах, семейное положение, СНИЛС, состав семьи, социальное положение, степень родства, судимость, трудоспособность, фамилия, имя, отчество, фотография.

4) члены профсоюза:

Иные категории ПДн: адрес, год рождения, дата рождения, занимаемая должность, контактные сведения, образование, профессия, фамилия, имя, отчество, фотография.

Способ обработки персональных данных: смешанный тип обработки персональных данных со следующими действиями с персональными данными: запись; извлечение; использование; накопление; передача (доступ); передача (предоставление); передача (распространение); сбор; систематизация; удаление; уничтожение; уточнение (обновление, изменение); хранение.

Срок обработки ПДн: 50 лет, срок хранения ПДн: 50 лет.

4. Правила обработки персональных данных

Все ПДн субъектов Бюджетное учреждение получает от них самих либо от их представителей или от сторонних организаций в рамках поручения (передачи) обработки ПДн субъектов Бюджетному учреждению.

Необходимые для ведения кадрового учёта ПДн ближайших родственников сотрудников, Бюджетное учреждение получает от самих сотрудников.

Обработка ПДн осуществляется на законной и справедливой основе, а также с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ на основании согласия субъекта ПДн на обработку его ПДн, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Типовая форма согласия субъекта ПДн приведена в приложении 2 к Правилам. Допускается совмещение формы согласия субъекта ПДн с типовыми формами документов, содержащих ПДн субъекта (например: анкеты, бланки).

Обработка ПДн ограничивается достижением конкретных, заранее определённых и законных целей. Обработке подлежат только ПДн, которые отвечают целям их обработки. Содержание и объём обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки. Не допускается обработка ПДн, несовместимая с целями сбора ПДн. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

При обработке ПДн Бюджетное учреждение обеспечивает точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Бюджетное учреждение принимает необходимые меры

либо обеспечивает их принятие по удалению или уточнению неполных или неточных данных.

Субъект ПДн принимает решение о предоставлении своих ПДн и даёт согласие на их обработку свободно, своей волей и в своём интересе. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. В случаях, предусмотренных федеральным законом, обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку своих ПДн, Бюджетное учреждение вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ, возлагается на Бюджетное учреждение.

Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку ПДн от представителя субъекта ПДн, полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Бюджетным учреждением.

В случае недееспособности субъекта ПДн, согласие на обработку его ПДн даёт законный представитель субъекта ПДн.

В случае смерти субъекта ПДн, согласие на обработку его ПДн дают наследники субъекта ПДн, если такое согласие не было дано субъектом ПДн при его жизни.

Бюджетное учреждение оставляет за собой право не осуществлять свои функции в отношении субъекта ПДн, в случае предоставления неполных или недостоверных ПДн, а также, в случае отказа дать письменное согласие на обработку ПДн на основании федерального закона.

Если в соответствии с федеральным законом предоставление ПДн и (или) получение Бюджетным учреждением согласия на обработку ПДн являются обязательными, Бюджетное учреждение обязано разъяснить субъекту ПДн

юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку.

При установлении договорных отношений с субъектом ПДн, получение письменного согласия на обработку его ПДн не требуется.

Получение ПДн субъекта у третьих лиц, возможно только при уведомлении субъекта ПДн об этом заранее и (или) с его письменного согласия. Типовая форма согласия субъекта на получение его ПДн у третьей стороны приведена в приложении 3 к Правилам. Допускается совмещение формы согласия субъекта ПДн с типовыми формами документов, содержащих ПДн субъекта (например: анкеты, бланки).

Бюджетное учреждение освобождается от обязанностей уведомлять субъекта ПДн, если его ПДн были получены Бюджетным учреждением у третьих лиц, в случаях, если:

1) субъект ПДн уведомлён об осуществлении обработки его ПДн Бюджетным учреждением соответствующим оператором;

2) персональные данные получены Бюджетным учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн;

3) обработка ПДн, разрешённых субъектом ПДн для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьёй 10.1 Федерального закона № 152-ФЗ;

4) Бюджетное учреждение осуществляет обработку ПДн для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта ПДн;

5) предоставление субъекту ПДн сведений, предусмотренных частью 3 статьи 18 Федерального закона № 152-ФЗ, нарушает права и законные интересы третьих лиц.

Бюджетным учреждением могут быть получены ПДн от лица, не являющегося субъектом ПДн, при условии предоставления Бюджетного учреждения подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

Бюджетное учреждение обрабатывает ПДн субъектов в структурных подразделениях (отделах) в соответствии с исполняемыми ими функциями и обязанностями.

Доступ к ПДн, обрабатываемым без использования средств автоматизации, осуществляется в соответствии с утверждённым списком допущенных лиц, утверждённым в порядке, определённом в Бюджетном учреждении.

Доступ к ПДн, обрабатываемым в информационных системах ПДн, осуществляется в соответствии с утверждённым Бюджетным учреждением списком лиц, утверждённым в порядке, определённом в Бюджетном учреждении.

Уполномоченные лица, допущенные к ПДн субъектов Бюджетного учреждения, имеют право получать только те ПДн субъекта(-ов), которые им необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями указанных лиц.

Обработка ПДн, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» утверждённого постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

При такой обработке, ПДн должны обособляться от иной другой информации, в частности, путём фиксации их на отдельных материальных носителях ПДн, в специальных разделах или на полях форм (бланков).

Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключаяющие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Бюджетным учреждением. Места хранения определяются отдельным приказом об утверждении мест хранения материальных носителей, перечня лиц ответственных за сохранность и доступ к ПДн Бюджетного учреждения.

Персональные данные могут подлежать блокированию, уточнению, уничтожению либо обезличиванию в одном из следующих случаев:

1) выявление неправомерной обработки ПДн при обращении либо по запросу субъекта ПДн или его представителя субъекта ПДн либо уполномоченного органа по защите прав субъектов ПДн (далее – уполномоченный орган);

2) выявление неточных ПДн при обращении либо по запросу субъекта ПДн или его представителя или по запросу уполномоченного органа;

3) выявление неправомерной обработки ПДн, осуществляемой Бюджетным учреждением или лицом, действующим по поручению Бюджетного учреждения и невозможности обеспечить правомерную обработку ПДн;

4) установление факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъекта(-ов) ПДн;

5) достижение целей обработки ПДн или в случае утраты необходимости в их достижении;

6) отзыв согласия субъекта ПДн на обработку его ПДн;

7) предоставление субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными, неактуальными (устаревшими), незаконно полученными или не являются необходимыми для заявленной цели обработки.

В случае выявления неправомерной обработки ПДн, при обращении либо по запросу субъекта ПДн или его представителя либо уполномоченного органа, Бюджетное учреждение осуществляет блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных ПДн, при обращении либо по запросу субъекта ПДн или его представителя либо по запросу уполномоченного органа, Бюджетное учреждение осуществляет блокирование ПДн, относящихся к этому субъекту ПДн, или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта ПДн или третьих лиц.

В случае подтверждения факта неточности ПДн, Бюджетное учреждение на основании сведений, предоставленных субъектом ПДн или его

представителем либо уполномоченным органом, или иных необходимых документов, уточняет ПДн либо обеспечивает их уточнение (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование ПДн.

В случае выявления неправомерной обработки ПДн, осуществляемой Бюджетным учреждением или лицом, действующим по поручению Бюджетного учреждения, Бюджетное учреждение в срок, не превышающий 3-х рабочих дней с даты этого выявления, осуществляет прекращение неправомерной обработки ПДн или обеспечивает прекращение неправомерной обработки ПДн лицом, действующим по поручению Бюджетного учреждения.

В случае, если обеспечить правомерность обработки ПДн невозможно, Бюджетное учреждение в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки ПДн, осуществляет уничтожение таких ПДн или обеспечивает их уничтожение. Решение о неправомерности обработки ПДн и необходимости уничтожения ПДн принимает ответственный за организацию обработки ПДн Бюджетного учреждения, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении ПДн Бюджетное учреждение уведомляет субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа были направлены уполномоченным органом, также указанный орган.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъекта(-ов) ПДн, Бюджетное учреждение с момента выявления такого инцидента Бюджетным учреждением, уполномоченным органом по защите прав субъектов ПДн или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов ПДн:

1) в течение 24-х часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемой вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Бюджетным учреждением на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;

2) в течение 72-х часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

В случае достижения цели обработки ПДн, Бюджетное учреждение прекращает обработку ПДн или обеспечивает её прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) и уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) в срок, не превышающий 30 дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Бюджетным учреждением и субъектом ПДн либо, если Бюджетное учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае отзыва субъектом ПДн согласия на обработку его ПДн, Бюджетное учреждение прекращает их обработку или обеспечивает прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожает ПДн или обеспечивает их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Бюджетным учреждением и субъектом ПДн либо, если Бюджетное учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае обращения субъекта ПДн к Бюджетному учреждению с требованием о прекращении обработки ПДн, Бюджетное учреждение в срок, не превышающий 10 рабочих дней с даты получения Бюджетным учреждением соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 – 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона № 152-ФЗ. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Бюджетным учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Бюджетное учреждение вносит в них необходимые изменения.

В срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Бюджетное учреждение уничтожает такие ПДн. При этом Бюджетное учреждение уведомляет субъекта ПДн или его представителя о внесённых изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанные выше по тексту, Бюджетное учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) и обеспечивает уничтожение ПДн в срок, не более, чем 6 месяцев, если иной срок не установлен федеральными законами.

Подтверждение уничтожения ПДн осуществляется в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов ПДн.

В случае, если обработка ПДн осуществляется Бюджетным учреждением без использования средств автоматизации, документом, подтверждающим уничтожение ПДн субъекта(-ов) ПДн, является акт об уничтожении ПДн. Типовая форма акта уничтожения ПДн приведена в приложении 4 к Правилам.

В случае, если обработка ПДн осуществляется Бюджетным учреждением с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъекта(-ов) ПДн, являются акт об уничтожении ПДн и выгрузка из журнала регистрации событий в информационной системе ПДн (далее – выгрузка из журнала).

Выгрузка из журнала должна содержать:

- а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи ПДн были уничтожены;
- б) перечень категорий уничтоженных ПДн субъекта(-ов) ПДн;
- в) наименование информационной системы ПДн, из которой были уничтожены ПДн субъекта(-ов) ПДн;
- г) причину уничтожения ПДн;

д) дату уничтожения ПДн субъекта(-ов) ПДн.

В случае, если выгрузка из журнала не позволяет указать отдельные сведения (указанные выше), недостающие сведения вносятся в акт об уничтожении ПДн.

В случае, если обработка ПДн осуществляется Бюджетным учреждением одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов ПДн, являются акт об уничтожении ПДн и выгрузка из журнала.

Акт(-ы) об уничтожении ПДн и выгрузка из журнала подлежат хранению в течение 3-х лет с момента уничтожения ПДн.

Уничтожение ПДн осуществляет комиссия в составе руководителя и сотрудников структурного подразделения (отдела), обрабатывавшего ПДн субъекта и установившего необходимость уничтожения ПДн под контролем руководителя этого структурного подразделения (отдела).

Способ уничтожения материальных носителей ПДн определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) уничтожение специализированной организацией;
- 5) химическая обработка.

При необходимости уничтожения большого количества материальных носителей, содержащих ПДн субъекта(-ов) или применения специальных способов уничтожения, допускается привлечение специализированных организаций. В этом случае, комиссия Бюджетного учреждения должна присутствовать при уничтожении материальных носителей ПДн. При этом, к акту уничтожения, необходимо приложить накладную на передачу материальных носителей ПДн, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных Бюджетного учреждения, содержащих ПДн субъекта(-ов), выполняется по заявке руководителя структурного подразделения (отдела), обрабатывавшего ПДн субъекта и установившего необходимость их уничтожения.

Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, сотрудники структурного подразделения (отдела),

обрабатывавшие ПДн субъекта(-ов) и установившие необходимость их уничтожения.

Уничтожение достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего в дальнейшем произвести считывание или восстановление ПДн. При этом составляется акт(-ы) об уничтожении ПДн и выгрузка из журнала. Типовая форма акта уничтожения ПДн приведена в приложении 4 к Правилам.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и (или) договорными документами.

При отсутствии технической возможности осуществить уничтожение ПДн, содержащихся в базах данных и (или) невозможности осуществления затирания информации на носителях, допускается проведение обезличивания путём перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта(-ов) ПДн была невозможна.

Контроль выполнения процедур уничтожения ПДн осуществляет ответственный за организацию обработки ПДн в Бюджетном учреждении. Бюджетное учреждение уведомляет субъекта ПДн или его представителя об уничтожении ПДн. Типовая форма уведомления об уничтожении ПДн субъекта приведена в приложении 5 к Правилам.

Особенности обработки специальных категорий ПДн, а также сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн), установлены соответственно статьями 10 и 11 Федерального закона № 152-ФЗ.

Обработка специальных категорий ПДн, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 Федерального закона № 152-ФЗ. Обработка ПДн о судимости может осуществляться государственными или муниципальными органами, в пределах полномочий, предоставленных им в соответствии с законодательством Российской Федерации, а также иными лицами, в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка биометрических ПДн может осуществляться только при наличии согласия в письменной форме субъекта ПДн, за исключением случаев,

предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ . Бюджетное учреждение не вправе отказывать в обслуживании в случае отказа субъекта ПДн предоставить биометрические ПДн и (или) дать согласие на обработку ПДн, если в соответствии с федеральным законом получение Бюджетным учреждением согласия на обработку ПДн не является обязательным. Типовая форма согласия субъекта на обработку его биометрических ПДн приведена в приложении 6 к Правилам. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих ПДн субъекта (например: анкеты, бланки).

Решение, порождающее юридические последствия в отношении субъекта ПДн или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его ПДн только при наличии согласия в письменной форме субъекта ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.

Запрещается принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы.

Бюджетное учреждение разъясняет субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставляет возможность субъекту ПДн заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.

Бюджетное учреждение рассматривает возражение в течение 30 дней со дня его получения и уведомляет субъекта ПДн о результатах рассмотрения такого возражения.

Сотрудники Бюджетного учреждения должны быть ознакомлены под роспись с требованиями законодательства Российской Федерации, касающимися обработки ПДн, настоящими Правилами и другими документами Бюджетного учреждения, устанавливающими порядок обработки ПДн субъектов, а также права и обязанности в этой области.

5. Правила работы с обезличенными данными

Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), как уполномоченным органом по защите прав субъектов ПДн в Российской Федерации, установлены

требования и методы по обезличиванию ПДн, обрабатываемых в информационных системах, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утверждены Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Методические рекомендации содержат анализ процессов автоматизированной обработки обезличенных данных, требования к обезличенным данным и методам обезличивания, позволяющие выделить основные свойства обезличенных данных и методы обезличивания, и оценить возможность их применения при решении задач обработки ПДн с учётом вида деятельности Оператора и необходимых действий с ПДн.

К наиболее перспективным и удобным для практического применения обезличивания, относится один из следующих методов:

1) метод введения идентификаторов (замена части сведений (значений ПДн) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);

2) метод изменения состава или семантики (изменение состава или семантики ПДн путём замены результатами статистической обработки, обобщения или удаления части сведений);

3) метод декомпозиции (разбиение множества (массива) ПДн на несколько подмножеств (частей) с последующим отдельным хранением подмножеств);

4) метод перемешивания (перестановка отдельных записей, а также групп записей в массиве ПДн).

Обезличивание должно проводиться таким образом, чтобы определить принадлежность ПДн конкретному субъекту ПДн было невозможно без использования дополнительной информации.

В случае, если обезличенные ПДн используются в статистических или иных исследовательских целях, сроки обработки и хранения ПДн устанавливаются руководством Бюджетного учреждения исходя из служебной необходимости, и получение согласия субъекта на обработку его ПДн не требуется, на основании пункта 9 части 1 статьи 6 Федерального закона № 152-ФЗ.

Если обезличенные ПДн используются в целях продвижения товаров, работ, услуг на рынке, или в целях политической агитации, Бюджетное учреждение обязано получить согласие субъекта ПДн на подобную обработку.

Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных ПДн в информационных системах и целесообразность их применения определяются ответственным за организацию обработки ПДн Бюджетного учреждения для каждой информационной системы с ПДн индивидуально.

6. Передача персональных данных третьим лицам

При обработке ПДн субъекта должны соблюдаться следующие требования:

1) не сообщать ПДн субъекта третьей стороне без письменного согласия субъекта. Типовая форма согласия субъекта на передачу его ПДн третьей стороне приведена в приложении 7 к Правилам. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими ПДн субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152;

2) предупреждать лиц, получающих ПДн субъекта(-ов), 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 ПДн субъекта(-ов), обязаны соблюдать режим конфиденциальности в отношении этих данных.

Бюджетное учреждение до начала осуществления деятельности по трансграничной передаче ПДн уведомляет уполномоченный орган по защите прав субъектов ПДн о своём намерении осуществлять трансграничную передачу ПДн. Данное уведомление направляется отдельно от уведомления о намерении осуществлять обработку ПДн, предусмотренного статьей 22 Федерального закона № 152-ФЗ. До подачи такого уведомления Бюджетное учреждение получает от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача ПДн, сведения, предусмотренные частью 5 статьи 12 Федерального закона № 152.

После направления уведомления, Бюджетное учреждение вправе осуществлять трансграничную передачу ПДн на территории указанных в таком уведомлении иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн (далее – Конвенция) или включённых в перечень не являющихся сторонами Конвенции, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер

по обеспечению конфиденциальности и безопасности персональных данных при их обработке – до принятия решения, указанных в части 8 или 12 статьи 12 Федерального закона № 152.

В целях оценки достоверности сведений, содержащихся в уведомлении Бюджетного учреждения о своём намерении осуществлять трансграничную передачу ПДн, Бюджетным учреждением предоставляются сведения, предусмотренные пунктами 1 - 3 части 5 статьи 12 Федерального закона № 152 по запросу уполномоченного органа по защите прав субъектов ПДн в течение 10 рабочих дней с даты получения такого запроса. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Бюджетным учреждением в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Трансграничная передача ПДн может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства, защиты экономических и финансовых интересов Российской Федерации, обеспечения дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других её интересов на международной арене с даты принятия уполномоченным органом по защите прав субъектов ПДн решения, предусмотренного частью 12 статьи 12 Федерального закона № 152.

Решение о запрещении или об ограничении трансграничной передачи ПДн в целях защиты нравственности, здоровья, прав и законных интересов граждан принимается уполномоченным органом по защите прав субъектов ПДн по результатам рассмотрения уведомления. Данное решение принимается в течение 10 рабочих дней с даты поступления уведомления в уполномоченный орган по защите прав субъектов ПДн. В случае направления в адрес Бюджетного учреждения уполномоченным органом по защите прав субъектов ПДн запроса оценки достоверности сведений, предусмотренные пунктами 1 - 3 части 5 статьи 12 Федерального закона № 152, рассмотрение уведомления о намерении осуществлять трансграничную передачу ПДн приостанавливается до даты предоставления Бюджетным учреждением запрошенной информации.

После направления уведомления, Бюджетное учреждение до истечения сроков указанных в предыдущем абзаце, не вправе осуществлять трансграничную передачу ПДн на территории указанных в уведомлении иностранных государств, не являющихся сторонами Конвенции и не

включённых в перечень, за исключением случая, если такая трансграничная передача ПДн необходима для защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц.

В случае принятия уполномоченным органом по защите прав субъектов ПДн решения, предусмотренного частью 8 или 12 статьи 12 Федерального закона № 152, Бюджетное учреждение обеспечивает уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им ПДн.

Правительство Российской Федерации определяет случаи, при которых требования частей 3 - 6, 8 - 11 настоящей статьи не применяются к операторам, осуществляющим трансграничную передачу персональных данных в целях выполнения возложенных международным договором Российской Федерации, законодательством Российской Федерации на государственные органы, муниципальные органы функций, полномочий и обязанностей.

7. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

Согласие на обработку ПДн, разрешённых субъектом ПДн для распространения, оформляется отдельно от иных согласий субъекта ПДн на обработку его ПДн. Бюджетное учреждение обеспечивает субъекту ПДн возможность определить перечень ПДн по каждой категории ПДн, указанной в согласии на обработку ПДн, разрешённых субъектом ПДн для распространения. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом ПДн для распространения, устанавливаются уполномоченным органом по защите прав субъектов ПДн. Типовая форма согласия субъекта на обработку персональных данных, разрешенных субъектом персональных данных для распространения приведена в приложении 8 к Правилам.

В случае раскрытия ПДн неопределённому кругу лиц самим субъектом ПДн без предоставления Бюджетному учреждению согласия, предусмотренного требованием Федерального закона № 152-ФЗ, обязанность предоставить доказательства законности последующего распространения или иной обработки таких ПДн лежит на каждом лице, осуществившем их распространение или иную обработку.

В случае, если ПДн оказались раскрытыми неопределённому кругу лиц вследствие правонарушения, преступления или обстоятельств непреодолимой силы, обязанность предоставить доказательства законности последующего

распространения или иной обработки таких ПДн лежит на каждом лице, осуществившем их распространение или иную обработку.

В случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешённых субъектом ПДн для распространения, не следует, что субъект ПДн согласился с распространением ПДн, такие ПДн обрабатываются Бюджетным учреждением, которому они предоставлены субъектом ПДн, без права распространения.

В случае, если из предоставленного субъектом ПДн согласия на обработку ПДн, разрешённых субъектом ПДн для распространения, не следует, что субъект ПДн не установил запреты и условия на обработку ПДн, предусмотренные частью 9 статьи 10.1 Федерального закона № 152-ФЗ, или если в предоставленном субъектом ПДн таком согласии не указаны категории и перечень ПДн, для обработки которых субъект ПДн устанавливает условия и запреты в соответствии с частью 9 статьи 10.1 Федерального закона № 152-ФЗ, такие ПДн обрабатываются Бюджетным учреждением, которому они предоставлены субъектом ПДн, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с ПДн неограниченному кругу лиц.

Согласие на обработку ПДн, разрешённых субъектом ПДн для распространения, может быть предоставлено Бюджетному учреждению:

- 1) непосредственно;
- 2) с использованием информационной системы уполномоченного органа по защите прав субъектов ПДн.

Правила использования информационной системы уполномоченного органа по защите прав субъектов ПДн, в том числе порядок взаимодействия субъекта ПДн с Бюджетным учреждением, определяются уполномоченным органом по защите прав субъектов ПДн.

Молчание или бездействие субъекта ПДн ни при каких обстоятельствах не может считаться согласием на обработку ПДн, разрешённых субъектом ПДн для распространения.

В согласии на обработку ПДн, разрешённых субъектом ПДн для распространения, субъект ПДн вправе установить запреты на передачу (кроме предоставления доступа) этих ПДн Бюджетным учреждением неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих ПДн неограниченным кругом лиц. Отказ Бюджетного учреждения в установлении субъектом ПДн запретов и условий, предусмотренных статьёй 10.1 Федерального закона № 152-ФЗ, не допускается.

Бюджетное учреждение в срок, не позднее 3-х рабочих дней с момента получения соответствующего согласия субъекта ПДн, опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПДн, разрешённых субъектом ПДн для распространения.

Установленные субъектом ПДн запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) ПДн, разрешённых субъектом ПДн для распространения, не распространяются на случаи обработки ПДн в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

Передача (распространение, предоставление, доступ) ПДн, разрешённых субъектом ПДн для распространения, должна быть прекращена в любое время по требованию субъекта ПДн. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта ПДн, а также перечень ПДн, обработка которых подлежит прекращению. Указанные в данном требовании ПДн могут обрабатываться только Бюджетным учреждением, которому оно направлено.

Действие согласия субъекта ПДн на обработку ПДн, разрешённых субъектом ПДн для распространения, прекращается с момента поступления Бюджетному учреждению требования о прекращении данной обработки или определённого перечня ПДн указанного в согласии.

Субъект ПДн вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих ПДн, ранее разрешённых субъектом ПДн для распространения, к любому лицу, обрабатывающему его ПДн, в случае несоблюдения положений статьи 10.1 Федерального закона № 152-ФЗ или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) ПДн в течение трёх рабочих дней с момента получения требования субъекта ПДн или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трёх рабочих дней с момента вступления решения суда в законную силу.

Требования статьи 10.1 Федерального закона № 152-ФЗ не применяются в случае обработки ПДн в целях выполнения возложенных законодательством Российской Федерации на государственные органы, муниципальные органы, а также на подведомственные таким органам организации функций, полномочий и обязанностей.

8. Права субъектов персональных данных

В целях обеспечения своих законных интересов, субъекты ПДн или его представители имеют право:

1) получать полную информацию о своих ПДн и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, содержащей ПДн субъекта, за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона № 152-ФЗ;

3) требовать уточнение своих ПДн, их блокирование или уничтожение, в случаях, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав. Субъект ПДн при отказе Бюджетного учреждения исключить или исправить, заблокировать или уничтожить его ПДн, имеет право заявить в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие;

4) требовать от Бюджетного учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные, устаревшие, неточные, незаконно полученные или не являющиеся необходимыми для заявленной цели обработки ПДн субъекта, обо всех произведённых в них изменениях или исключениях из них, в том числе блокирование или уничтожение этих данных третьими лицами;

5) обжаловать в суде или в уполномоченном органе по защите прав субъектов ПДн любые неправомерные действия или бездействие Бюджетного учреждения при обработке и защите ПДн субъекта, если субъект ПДн считает, что Бюджетное учреждение осуществляет обработку его ПДн с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы. Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

В случае, если обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Бюджетное учреждение или направить ему повторный запрос в целях получения сведений, и ознакомления с ПДн не ранее, чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в

соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

Субъект ПДн вправе обратиться повторно или направить ему повторный запрос до истечения 30 дневного срока в случае, если сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Бюджетное учреждение вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренные частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Бюджетном учреждении.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами.

9. Порядок действий, в случае запроса уполномоченного органа по защите прав субъектов персональных данных

В соответствии с частью 4 статьи 20 Федерального закона № 152, Бюджетное учреждение сообщает в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 10 дней с даты получения такого запроса. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Бюджетным учреждением в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки ПДн Бюджетного учреждения, при необходимости с привлечением сотрудников Бюджетного учреждения.

В течение установленного законодательством срока, ответственный за организацию обработки ПДн Бюджетного учреждения подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

10. Защита персональных данных субъекта

Защиту ПДн субъектов от неправомерного их использования или утраты Бюджетное учреждение обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке ПДн должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты ПДн при их обработке техническими средствами устанавливаются в соответствии с:

1) приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

2) приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

3) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утверждённые приказом Гостехкомиссии России от 30 августа 2002 г. № 282;

4) внутренними документами Бюджетного учреждения, действующими в сфере обеспечения информационной безопасности.

Защита ПДн предусматривает ограничение к ним доступа.

Руководитель структурного подразделения (отдела) Бюджетного учреждения, осуществляющего обработку ПДн:

1) несёт ответственность за организацию защиты ПДн в подчинённом структурном подразделении (отделе);

2) закрепляет за сотрудниками, уполномоченными обрабатывать ПДн, конкретные материальные носители, на которых допускается хранение ПДн в случае, если такие носители необходимы для выполнения возложенных на сотрудников функций и задач;

3) обеспечивает изучение уполномоченными сотрудниками, в чьи обязанности входит обработка ПДн, нормативных правовых актов по защите ПДн и требует их неукоснительного исполнения;

4) обеспечивает режим конфиденциальности в отношении ПДн, обрабатываемых в структурном подразделении (отделе);

5) контролирует порядок доступа к ПДн, в соответствии с функциональными обязанностями (должностными обязанностями,

регламентами, положениями) сотрудников структурного подразделения (отдела).

Сотрудники Бюджетного учреждения, допущенные к обработке ПДн, дают письменное обязательство о неразглашении таких данных.

11. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с ПДн, обязаны:

- 1) знать законодательство Российской Федерации в области обработки и защиты ПДн, нормативные документы Бюджетного учреждения по обработке и защите ПДн;
- 2) сохранять конфиденциальность ПДн;
- 3) обеспечивать сохранность закреплённых за ними носителей ПДн;
- 4) контролировать срок истечения действия согласий на обработку ПДн и, при необходимости дальнейшей обработки ПДн, обеспечивать своевременное получение новых согласий или прекращение обработки ПДн;
- 5) докладывать своему непосредственному руководителю структурного подразделения (отдела) обо всех фактах и попытках несанкционированного доступа к ПДн и других нарушениях.

Ответственный за организацию обработки ПДн Бюджетного учреждения организует проведение инструктажа и ознакомление сотрудников Бюджетного учреждения, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Бюджетного учреждения в отношении обработки ПДн, локальными актами по вопросам обработки ПДн.

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

Лица, виновные в нарушении норм, регулирующих получение, обработку, передачу и защиту ПДн субъекта(-ов), привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;

3) увольнение.

За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

Копия приказа о применении к сотруднику дисциплинарного взыскания с указанием оснований его применения вручается сотруднику под расписку в течение 5 дней со дня издания приказа.

Если, в течение года со дня применения дисциплинарного взыскания сотрудник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Бюджетное учреждение, до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с сотрудника по собственной инициативе, по письменному заявлению сотрудника или по ходатайству его непосредственного руководителя структурного подразделения (отдела).

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 1
к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

Дополнительное соглашение № _____
к договору (контракту) от _____ № _____

г. Армавир

«___» _____ 20__ года

Государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края, в лице и.о. главного врача Фурсенко С.А., действующего на основании Устава, именуемое в дальнейшем «Заказчик», с одной стороны, и _____, в лице _____, действующего на основании _____, именуемое в дальнейшем «Исполнитель», с другой стороны, совместно именуемые «Стороны», заключили настоящее дополнительное соглашение о нижеследующем:

Дополнить договор (контракт) от _____ № _____ разделом следующего содержания:

1. Заказчик, являющийся, согласно Федеральному закону Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), оператором персональных данных, поручает Исполнителю обработку персональных данных.

2. Исполнитель является лицом, обрабатывающим персональные данные по поручению Заказчика.

3. Обработка персональных данных по поручению Заказчика, производится Исполнителем с целью:

(указать цели обработки)

4. Перечень действий (операций) по обработке персональных данных, которые будут совершаться лицом, осуществляющим обработку персональных данных, в рамках поручения:

(указать перечень действий)

5. Исполнитель вправе осуществлять обработку следующих персональных данных субъекта(-ов) по поручению Заказчика:

(указать категории персональных данных)

Конфиденциальность и безопасность персональных данных.

1. Вся предоставляемая Сторонами друг другу информация считается конфиденциальной и не подлежит разглашению третьим лицам.

2. Исполнитель обязуется осуществлять обработку персональных данных субъекта(-ов) Заказчика в соответствии с принципами и правилами обработки персональных данных, предусмотренных Федеральным законом № 152-ФЗ.

3. Исполнитель обязуется соблюдать конфиденциальность полученных персональных данных субъекта(-ов) Заказчика и обеспечить безопасность персональных данных при их обработке.

4. Исполнитель при обработке персональных данных субъекта(-ов) Заказчика обязуется принимать все необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

Исполнитель при обработке персональных данных по поручению Заказчика обязан принимать меры, необходимые и достаточные для выполнения обязанностей, предусмотренных законодательством Российской Федерации, предусмотренные ст. 18.1 Федерального закона № 152-ФЗ:

1) назначить ответственного за организацию обработки персональных данных;

2) издать документы, определяющие политику в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также документ, устанавливающий процедуры, направленный на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных,

политике Исполнителя в отношении обработки персональных данных, локальным актам Исполнителя;

4) проводить оценку вреда, в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, а также оценивать соотношение указанного вреда и принимаемых Исполнителем мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

5) ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Исполнителя в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) провести обучение указанных работников.

5. Исполнитель обязуется обеспечить безопасность персональных данных применением таких мер как:

1) определить угрозы безопасности персональных данных, если они будут обрабатываться в информационных системах персональных данных Исполнителя;

2) применять организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применять прошедшие в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценивать эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) вести учет машинных носителей персональных данных, если порученные на обработку персональные данные будут на них фиксироваться Исполнителем;

6) обнаруживать факты несанкционированного доступа к персональным данным, порученным на обработку, и принимать, в связи с этим необходимые

меры по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

8) устанавливать правила доступа к персональным данным, которые поручены на обработку и обрабатываются в информационных системах персональных данных Исполнителя, а также обеспечивать регистрацию и учет всех действий, совершаемых с персональными данными в информационной системе персональных данных Исполнителя;

9) осуществлять контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных, в которых обрабатываются порученные на обработку персональные данные.

6. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Исполнитель обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

7. Стороны принимают все необходимые меры для того, чтобы предотвратить разглашение получаемой информации в рамках настоящего договора (контракта). Информация может быть предоставлена третьим лицам только в порядке, установленном действующим законодательством Российской Федерации.

8. В течение всего срока действия данного соглашения Заказчик вправе запросить, а Исполнитель обязан предоставить в течение 7 рабочих дней с момента получения запроса от Заказчика информацию (включая документы), подтверждающую принятие мер и соблюдение в целях исполнения поручения Заказчика требований, установленных данным соглашением и законодательством Российской Федерации.

9. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Исполнитель обязан с момента выявления такого инцидента уведомить Заказчика:

1) в течение рабочего дня с момента обнаружения данного факта: о произошедшем инциденте; о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных; о предполагаемой вреде, нанесенном правам субъектов персональных данных; о принятых мерах по устранению последствий соответствующего инцидента; предоставить сведения о лице, уполномоченным Исполнителем на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленными инцидентами;

2) в течение 48-ми часов с момента выявленного факта: о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

10. Исполнитель по запросу Заказчика должен уничтожить определенные Заказчиком или все персональные данные, которые были поручены ему на обработку, в течение 30 дней с момента получения запроса, если обработка их не требуется законодательству Российской Федерации.

В случае отсутствия возможности уничтожения персональных данных в течение 30 календарных дней с момента поступления запроса от Заказчика, Исполнитель осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок, не превышающий 6 месяцев. О факте блокирования Исполнитель сообщает Заказчику в срок, не превышающий 30 дней с момента поступления запроса от Заказчика.

В случае невозможности уничтожить персональные данные по запросу Заказчика в связи с необходимостью их обработки, связанной с исполнением требований законодательства Российской Федерации, Исполнитель направляет мотивированное обоснование о невозможности уничтожения или блокировки персональных данных Заказчику в срок, не превышающий 30 дней с момента поступления запроса от Заказчика.

11. Заказчик вправе в течение всего срока действия настоящего соглашения запрашивать у Исполнителя копии документов, подтверждающих уничтожение персональных данных, переданных ему на обработку. Копии документов должны быть предоставлены не позднее 5 рабочих дней с даты получения соответствующего запроса Заказчика.

12. Настоящее дополнительное соглашение является неотъемлемой частью договора (контракта) от _____ № _____, составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

13. Дополнительное соглашение вступает в силу с момента подписания настоящего соглашения Сторонами.

От Заказчика:

От Исполнителя:

(подпись) (И.О. Фамилия)

(подпись) (И.О. Фамилия)

« ____ » _____ 20 ____ г.

« ____ » _____ 20 ____ г.

М.П.

М.П.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 2

к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

И.о. главного врача
ГБУЗ Армавирского КВД

С.А. Фурсенко

СОГЛАСИЕ

**на обработку персональных данных сотрудника
государственное бюджетное учреждение здравоохранения
«Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края, иных
субъектов персональных данных**

Я, _____, проживающий(-ая) по
адресу _____,
паспорт серия _____, номер _____, выдан _____

«__» _____ года, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,
даю согласие государственному бюджетному учреждению здравоохранения
«Армавирский кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края (далее – Бюджетное учреждение),
расположенному по адресу 352905, Россия, Краснодарский край, г. Армавир, ул.
Кирова, д. 64, на обработку моих персональных данных, а именно:

(перечислить категории персональных данных)

а также специальные категории персональных данных и (или) биометрические
персональные данные:

(перечислить специальные категории персональных данных и (или) биометрические данные)

В целях:

(указать цели обработки)

Перечень допустимых действий, осуществляемых Бюджетным учреждением с персональными данными:

(перечислить перечень действий (операций) по обработке персональных данных)

а также передача следующих персональных данных:

(перечислить категории передаваемых персональных данных)

для обработки в целях:

(указать цели обработки)

следующим лицам:

(указать Ф.И.О., адрес физического лица или наименование и адрес организации, которым сообщаются данные)

Бюджетное учреждение может осуществлять:

(перечислить тип обработки и наличие передачи персональных данных)

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае, принятия Бюджетным учреждением решения о прекращении обработки персональных данных и (или) уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«___» _____ 20___ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 3
к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

И.о. главного врача
ГБУЗ Армавирского КВД

С.А. Фурсенко

СОГЛАСИЕ
субъекта на получение его персональных данных у третьей
стороны

Я, _____, проживающий(-ая) по
адресу _____,
паспорт серия _____, номер _____, выдан _____

«__» _____ года, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,
даю согласие государственному бюджетному учреждению здравоохранения
«Армавирский кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края (далее – Бюджетное учреждение),
расположенному по адресу 352905, Россия, Краснодарский край, г. Армавир, ул.
Кирова, д. 64, на получение моих персональных данных у третьей стороны, а
именно:

(указать третьих лиц)

Следующие персональные данные:

(перечислить категории персональных данных)

а также специальные категории персональных данных и (или) биометрические персональные данные:

(перечислить специальные категории персональных данных и (или) биометрические данные)

В целях:

(указать цели обработки)

Перечень допустимых действий, осуществляемых Бюджетным учреждением с персональными данными:

(перечислить перечень действий (операций) по обработке персональных данных)

Бюджетное учреждение может осуществлять:

(перечислить тип обработки и наличие передачи персональных данных)

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае, принятия Бюджетным учреждением решения о прекращении обработки персональных данных и (или) уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«___» _____ 20__ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 4

к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

АКТ № _____

об уничтожении персональных данных субъекта в
государственном бюджетном учреждении здравоохранения
«Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края

Состав комиссии:

Председатель комиссии:

_____ (должность) _____ (И.О. Фамилия)

Члены комиссии:

_____ (должность) _____ (И.О. Фамилия)

_____ (должность) _____ (И.О. Фамилия)

_____ (должность) _____ (И.О. Фамилия)

Комиссия произвела отбор к уничтожению следующих персональных
данных субъекта(-ов) персональных данных:

№ п/п	ФИО субъекта или иная информация, относящиеся к определенному физическому лицу	Перечень категорий персональных данных субъекта	Наименование материального носителя	Наименование информационной системы (при обработке)	Количество листов материального носителя
1	2	3	4	5	6

Причина уничтожения:

- ☐ достижение целей обработки персональных данных ☐ решение субъекта персональных данных ☐ недостоверные персональные данные

Всего подлежит уничтожению _____ (цифрами) (_____ (прописью))

наименований документов.

Документы уничтожены с помощью

(указать способ уничтожения)

Всего подлежит уничтожению _____ (_____)
 (цифрами) (прописью)

наименований полей баз данных из информационной системы.

Поля баз данных уничтожены с помощью:

(указать способ уничтожения)

Дата уничтожения персональных данных субъекта(-ов) персональных данных: _____.

Оператор обработки персональных данных (государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края), расположен по адресу: 352905, Россия, Краснодарский край, г. Армавир, ул. Кирова, д. 64.

Наименование юридического лица или фамилия, имя, отчество (при наличии) физического лица и адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъектов персональных данных по поручению Бюджетного учреждения:

(при необходимости)

Председатель комиссии:

(подпись)

(И.О. Фамилия)

Члены комиссии:

(подпись)

(И.О. Фамилия)

(подпись)

(И.О. Фамилия)

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 5
к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

УВЕДОМЛЕНИЕ
об уничтожении персональных данных субъекта

Уважаемый(-ая) _____

(Ф.И.О. субъекта персональных данных)

Обработка Ваших персональных данных прекращена.

Ваши персональные данные, которые обрабатывались в государственном
бюджетном учреждении здравоохранения «Армавирский
кожно-венерологический диспансер» министерства здравоохранения
Краснодарского края, были уничтожены.

Приложение: копия акта об уничтожении на _____ листе(-ах).

Ответственный за
организацию обработки
персональных данных
ГБУЗ Армавирского КВД

(должность)

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 6
к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

И.о. главного врача
ГБУЗ Армавирского КВД

С.А. Фурсенко

СОГЛАСИЕ
субъекта на обработку его биометрических персональных
данных

Я, _____, проживающий(-ая) по
адресу _____,
паспорт серия _____, номер _____, выдан _____

«__» _____ года, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,
даю согласие государственному бюджетному учреждению здравоохранения
«Армавирский кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края (далее – Бюджетное учреждение),
расположенному по адресу 352905, Россия, Краснодарский край, г. Армавир, ул.
Кирова, д. 64, на обработку моих биометрических персональных данных, а
именно:

(перечислить биометрические персональные данные)

В целях

(указать цели обработки)

Перечень допустимых действий, осуществляемых с персональными данными:

(перечислить перечень действий (операций) по обработке персональных данных)

Бюджетное учреждение может осуществлять:

(перечислить тип обработки и наличие передачи персональных данных)

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае, принятия Бюджетным учреждением решения о прекращении обработки персональных данных и (или) уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«__» _____ 20__ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 7
к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

И.о. главного врача
ГБУЗ Армавирского КВД

С.А. Фурсенко

СОГЛАСИЕ
субъекта на передачу его персональных данных третьей
стороне

Я, _____, проживающий(-ая) по
адресу _____,
паспорт серия _____, номер _____, выдан _____

«__» _____ года, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»,
даю согласие государственному бюджетному учреждению здравоохранения
«Армавирский кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края (далее – Бюджетное учреждение),
расположенному по адресу 352905, Россия, Краснодарский край, г. Армавир, ул.
Кирова, д. 64, на обработку моих персональных данных, а именно:

(перечислить категории персональных данных)

а также специальные категории персональных данных и (или) биометрические
персональные данные:

(перечислить специальные категории персональных данных и (или) биометрические данные)

Для обработки в целях

(указать цели обработки)

Следующим лицам

(указать Ф.И.О., адрес физического лица или наименование и адрес организации, которым сообщаются данные)

Перечень действий (операций) по обработке персональных данных, которые будут совершаться лицом, осуществляющим обработку персональных данных, в рамках согласия (поручения, договора):

(перечислить перечень действий (операций) по обработке персональных данных)

Третья сторона может осуществлять:

(перечислить тип обработки и наличие передачи персональных данных)

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в случае, принятия третьей стороной решения о прекращении обработки персональных данных и (или) уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«__» _____ 20__ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 8
к Правилам обработки
персональных данных субъектов
персональных данных в ГБУЗ
Армавирском КВД

И.о. главного врача
ГБУЗ Армавирского КВД

С.А. Фурсенко

СОГЛАСИЕ
субъекта на обработку персональных данных, разрешённых
субъектом персональных данных для распространения

Я, _____,
проживающий(-ая) по адресу:

_____, контактный номер телефона:
_____, адрес электронной почты:

_____, в соответствии с
Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О
персональных данных», даю согласие государственному бюджетному
учреждению здравоохранения «Армавирский кожно-венерологический
диспансер» министерства здравоохранения Краснодарского края (ИНН
2302018618), расположенному по адресу 352905, Россия, Краснодарский край, г.
Армавир, ул. Кирова, д. 64, код(ы) классификаторов по направлениям
деятельности:

ОКВЭД: _____,

ОКПО: _____,

ОКОГУ: _____,

ОКОП: _____,

ОКФС: _____,

на обработку моих персональных данных, разрешённых для распространения, а
именно:

(перечислить категории персональных данных)

и другие:

(перечислить дополнительные категории персональных данных)

В целях

(указать цели обработки)

Перечень допустимых действий, осуществляемых с персональными данными, разрешёнными для распространения:

(перечислить перечень действий (операций) по обработке персональных данных)

Государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение) может осуществлять обработку персональных данных, разрешённых для распространения:

(перечислить тип обработки и наличие передачи персональных данных)

Следующие мои персональные данные:

☐ не подлежат распространению

☐ подлежат распространению только при соблюдении следующих условий

Бюджетное учреждение осуществляет распространение персональных данных посредством ресурса/размещения на ресурсе [http\(s\)://](http(s)://) .

Согласие вступает в силу со дня его подписания и действует в течение _____. Действие настоящего согласия прекращается досрочно в _____.

случае принятия Бюджетным учреждением решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

«__» _____ 20__ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

УТВЕРЖДЕНЫ

приказом ГБУЗ Армавирского КВД

от 25.06.2024 № 305-17

ПРАВИЛА

рассмотрения запросов субъектов персональных данных или их представителей в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края

При устном обращении либо письменном запросе субъекта персональных данных (далее – ПДн) или его представителя на доступ к ПДн субъекта, государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение) руководствуется требованиями статей 14, 18 и 20 Федерального закона Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

Сведения о наличии и обработке ПДн предоставляются субъекту ПДн или его представителю Бюджетным учреждением при обращении либо при получении запроса от субъекта ПДн или его представителя в той форме, в которой направлено соответствующее обращение либо запрос, если иное не указано в самом обращении или запросе. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Бюджетным учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Бюджетным учреждением, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- 1) подтверждение факта обработки ПДн Бюджетным учреждением;
- 2) правовые основания и цели обработки ПДн;

- 3) цели и применяемые Бюджетным учреждением способы обработки ПДн;
- 4) наименование и место нахождения Бюджетного учреждения, сведения о лицах (за исключением сотрудников Бюджетного учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Бюджетным учреждением или на основании федерального закона;
- 5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- 6) сроки обработки ПДн, в том числе сроки их хранения;
- 7) порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом № 152-ФЗ;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Бюджетного учреждения, если обработка поручена или будет поручена такому лицу;
- 10) информацию о способах исполнения Бюджетным учреждением обязанностей, установленных статьёй 18.1 Федерального закона № 152-ФЗ;
- 11) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

Доступ субъекта ПДн или его представителя к ПДн субъекта Бюджетное учреждение предоставляет только под контролем ответственного за организацию обработки ПДн (далее – Ответственный) Бюджетного учреждения.

Обращение и (или) запрос субъекта ПДн или его представителя фиксируется в журнале учёта обращений и (или) запросов граждан по вопросам обработки ПДн. Рекомендуемая форма журнала приведена в приложении к данному документу.

Ответственный Бюджетного учреждения принимает решение о предоставлении доступа субъекту ПДн или его представителю к ПДн указанного субъекта.

В случае, если данные, предоставленные субъектом ПДн или его представителем не достаточны для установления его личности или предоставление ПДн нарушают конституционные права и свободы других лиц, Ответственный Бюджетного учреждения подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющийся основанием для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения субъекта

ПДн или его представителя либо от даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Бюджетным учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Для предоставления доступа субъекту ПДн или его представителя к ПДн субъекта, Ответственный Бюджетного учреждения привлекает сотрудников структурного подразделения (отдела), обрабатывающего ПДн субъекта, по согласованию с руководителем этого структурного подразделения (отдела).

Бюджетное учреждение предоставляет безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящиеся к этому субъекту ПДн. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Бюджетное учреждение осуществляет в них необходимые изменения. В срок, не превышающий 7 рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Бюджетное учреждение уничтожает такие ПДн. Бюджетное учреждение уведомляет субъекта ПДн или его представителя о внесённых изменениях и предпринятых мерах, и принимает разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанный выше по тексту, Бюджетное учреждение осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Бюджетного учреждения) и обеспечивает уничтожение ПДн в срок, не более, чем 6 месяцев, если иной срок не установлен федеральными законами.

Сведения о наличии ПДн Бюджетное учреждение предоставляет субъекту ПДн или его представителю в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Контроль предоставления сведений субъекту ПДн или его представителю осуществляет Ответственный Бюджетного учреждения.

Сведения о наличии ПДн должны быть предоставлены субъекту ПДн или его представителю при ответе на запрос или при обращении в течение 10 рабочих дней от даты получения запроса (обращения) субъекта ПДн или его представителя. Указанный срок может быть продлён, но не более чем на 5

рабочих дней в случае направления Бюджетным учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В случае отказа Бюджетным учреждением в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса субъекта ПДн или его представителя, Бюджетное учреждение предоставляет в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя. Указанный срок может быть продлён, но не более чем на 5 рабочих дней в случае направления Бюджетным учреждением в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами, в том числе, если:

1) обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

3) обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма;

4) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

5) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования

транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение
к Правилам рассмотрения запросов
субъектов персональных данных
или их представителей в ГБУЗ
Армавирском КВД

Государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края

ЖУРНАЛ
регистрации обращений и (или) запросов субъектов персональных данных
или их представителей по вопросам обработки персональных данных

Начат « ____ » ____ 20 ____ года Окончен « ____ » ____ 20 ____ года

(должность)

(должность)

/

(подпись)

(И.О. Фамилия)

/

(подпись)

(И.О. Фамилия)

/

На ____ листах

[illegible]

Заместитель главного врача по
экономическим
вопросам экономической службы

О.В. Белоноскина

Приложение 3

УТВЕРЖДЕНЫ

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ПРАВИЛА

**осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите
персональных данных, установленные Федеральным
законом «О персональных данных», принятыми в
соответствии с ним нормативными правовыми актами и
локальными актами в государственном бюджетном
учреждении здравоохранения «Армавирский
кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края**

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных (далее – ПДн) требованиям к защите ПДн в структурных подразделениях (отделах) государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение).

Правила обязательны для исполнения всеми должностными лицами Бюджетного учреждения, осуществляющими контроль состояния защиты ПДн.

Контроль выполнения соответствия обработки ПДн требованиям к защите ПДн в структурных подразделениях (отделах) Бюджетного учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты ПДн и его фактическим состоянием, правильности обработки ПДн ответственными лицами в структурных подразделениях (отделах), а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки ПДн (далее – Ответственный) в Бюджетном учреждении.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите ПДн и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты ПДн субъектов ПДн Бюджетного учреждения или нарушения требований по обработке и защите ПДн.

Проверки осуществляются Ответственным Бюджетного учреждения либо комиссией, образуемой и.о. главного врача.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых структурных подразделений (отделов).

Периодичность и сроки проведения плановых проверок структурных подразделений (отделов) Бюджетного учреждения устанавливаются планом, утверждаемый и.о. главного врача. Рекомендованная форма плана внутренних проверок состояния защиты ПДн приведена в приложении к данному документу. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа и утверждённого плана проверок и.о. главного врача. Ответственный Бюджетного учреждения подготавливает предложения по составу комиссии, при необходимости. Проект приказа о проверке подготавливает Ответственный Бюджетного учреждения.

Проверяющие лица (комиссия, при её наличии) и Ответственный Бюджетного учреждения обязаны получить у руководителей проверяемых структурных подразделений (отделов) информацию об условиях обработки ПДн, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения (отдела).

3. Порядок проведения проверки

По прибытию в структурное подразделение (отдел) для проведения проверки председатель комиссии (при наличии) или Ответственный Бюджетного учреждения прибывает к руководителю проверяемого структурного подразделения (отдела) Бюджетного учреждения, представляется ему и представляет других прибывших на проверку лиц (при наличии).

Руководитель проверяемого структурного подразделения (отдела) обязан оказывать содействие Ответственному Бюджетного учреждения и комиссии по проверке (при наличии) и в случае необходимости, определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку ПДн необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными ПДн.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите ПДн, выявление ответственных за обработку и защиту ПДн и установление факта ознакомления сотрудниками проверяемого структурного подразделения (отдела) со своей ответственностью;

2) получение при содействии сотрудников проверяемого структурного подразделения (отдела) документов, касающихся обработки и защиты ПДн в данном структурном подразделении (отделе);

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты ПДн и требований законодательства Российской Федерации в области защиты ПДн.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения (отдела) необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите ПДн в проверяемом структурном подразделении (отделе) Бюджетного учреждения рассматриваются, в частности, следующие показатели:

1) в части общей организации работ по обработке ПДн:

а) соответствие информации, указанной в уведомлении об обработке ПДн Бюджетного учреждения, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (ПДн), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Бюджетном учреждении;

в) наличие нормативных документов по защите ПДн;

г) знание нормативных документов сотрудниками, имеющими доступ к ПДн;

д) полнота и правильность выполнения требований нормативных документов сотрудниками Бюджетного учреждения, имеющими доступ к ПДн;

е) наличие документов, определяющих состав сотрудников, ответственных за обработку ПДн в структурном подразделении (отделе), соответствие этих документов реальному штатному составу структурного подразделения (отдела), а также подтверждение факта ознакомления ответственных сотрудников с данными документами;

ж) уровень подготовки сотрудников, ответственных за обработку ПДн в структурном подразделении (отделе);

з) наличие необходимых, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» согласий на обработку ПДн субъектов ПДн. Соответствие объёма обрабатываемых ПДн и сроков их обработки к указанным целям обработки ПДн.

2) в части защиты информационных систем с защищаемой информацией:

а) соответствие средств вычислительной техники, средств защиты информации и программного обеспечения в информационных системах показателям, указанным в документации на конкретную информационную систему (технический паспорт);

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) защищаемой информации в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники информационной системы;

г) наличие и эффективность применения средств и методов защиты информации, обрабатываемых на средствах вычислительной техники информационной системы;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы, средствам вычислительной техники, в том числе и BIOS;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта машинных носителей защищаемой информации. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к защищаемой информации;

б) правильность установления уровня защищённости ПДн в информационных системах ПДн и (или) правильности установления класса защищённости в государственных (муниципальных) информационных системах, при обработке в них ПДн;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности в правилах внутреннего трудового распорядка, положениях о структурных подразделениях (отделах) Бюджетного учреждения, должностных инструкциях и трудовых договорах сотрудников;

г) порядок передачи защищаемой информации органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих ПДн;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите ПДн должны быть по возможности устранены.

Проверяющие лица могут давать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

- 1) актом – при проведении проверки комиссией (при наличии);
- 2) служебной запиской – при проведении проверки Ответственным Бюджетного учреждения.

Акт и (или) служебная записка составляется в двух экземплярах и подписывается сотрудниками, выполнявшими проверку.

Один экземпляр хранится у Ответственного Бюджетного учреждения, второй экземпляр хранится в Бюджетном учреждении в установленном порядке. Копия документа о проверке остается у руководителя (начальника) проверяемого структурного подразделения (отдела).

Результаты проверок структурных подразделений (отделов) периодически обобщаются Ответственным Бюджетного учреждения и доводятся до руководителей структурных подразделений (отделов). При необходимости принятия решений по результатам проверок структурных подразделений (отделов) на имя и.о. главного врача готовятся соответствующие служебные записки.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите
персональных данных в ГБУЗ
Армави́рском КВД

ПЛАН
внутренних проверок состояния защиты персональных данных
государственного бюджетного учреждения здравоохранения «Армави́рский
кожно-венерологический диспансер» министерства здравоохранения
Краснодарского края
на 20__ год

№ п/п	Наименование структурного подразделения (отдела)	Квартал			
		I квартал	II квартал	III квартал	IV квартал
1	2	3	4	5	6
1					

(должность)

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 4

УТВЕРЖДЕН

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ПЕРЕЧЕНЬ
информационных систем персональных данных
государственного бюджетного учреждения здравоохранения
«Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края

Таблица 1

Перечень информационных систем персональных данных

№ п/п	Наименование ИСПДн	Класс ИСПДн	Уровень защищенности персональных данных	Применение СКЗИ для обеспечения безопасности ИСПДн
1	2	3	4	5
1	МИС "Медиалог"	ИСПДн-И	четвертый	Применяется
2	1С Предприятие 8.3: "Бухгалтерия"	ИСПДн-И	четвертый	Применяется
3	1С Предприятие 8.3: "Зарплата и кадры"	ИСПДн-С	третий	Не применяется
4	АРМ «Лаборатория» МИС «Ариадна»	ИСПДн-И	четвертый	Применяется

Таблица 2

Перечень государственных и(или) муниципальных
информационных систем

№ п/п	Наименование ГИС (МИС)	Уровень защищенности персональных данных (при наличии)	Класс защищенности ГИС (МИС)	Применение СКЗИ для обеспечения безопасности ГИС (МИС)
1	2	3	4	5
1	УРМ АС Бюджет	четвертый	третий (К 3)	Применяется

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

УТВЕРЖДЕНА

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ИНСТРУКЦИЯ
пользователя, допущенного к обработке персональных
данных в информационных системах государственного
бюджетного учреждения здравоохранения «Армавирский
кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края

1. Общие положения

Настоящий документ разработан на основе приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 г..

Настоящий документ определяет основные обязанности, права и ответственность пользователей, допущенных к обработке персональных данных в информационных системах (далее – ИС) государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение).

Допуск пользователей к обработке персональных данных (далее – ПДн) в ИС определяется приказом и.о. главного врача. Функционально пользователи ИС подчиняются своему непосредственному руководителю структурного подразделения (отдела) и по направлению обеспечения безопасности персональных данных ответственным за обеспечение безопасности и за организацию обработки ПДн Бюджетного учреждения.

Пользователь ИС руководствуется положениями федеральных законов и нормативных актов органов государственной власти, ведомственных организационно-распорядительных актов, нормативных актов Бюджетного учреждения, настоящей Инструкцией, а также другими распорядительными документами, в части его касающейся.

Внесение изменений в настоящую Инструкцию осуществляется на периодической и внеплановой основе. Внеплановое внесение изменений в настоящую Инструкцию может производиться в случае изменения действующего законодательства и иных нормативных актов в области обработки и обеспечения безопасности ПДн.

Контроль за выполнением требований настоящей Инструкции осуществляет ответственный за обеспечение безопасности ПДн в ИС (далее – Администратор ИБ).

2. Обязанности пользователя

При выполнении работ в ИС пользователь обязан:

1) строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, правила работы и порядок регистрации в ИС, доступа к информационным ресурсам ИС;

2) знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее – АРМ);

3) хранить в тайне свои идентификационные данные (имена, пароли и т. д.);

4) выполнять требования, предъявляемые к парольной системе (нормативы на длину, состав, периодичность смены пароля и т. д.), осуществлять вход на АРМ только под своими идентификационными данными;

5) передавать для хранения установленным порядком своё индивидуальное устройство идентификации, личную ключевую дискету и другие реквизиты разграничения доступа, только руководителю своего структурного подразделения (отдела) или Администратору ИБ;

6) выполнять требования «Инструкции по организации антивирусной защиты» в части, касающейся действий пользователей ИС;

7) немедленно вызывать Администратора ИБ и ставить в известность своего руководителя структурного подразделения (отдела) в случае утери персональной ключевой дискеты, индивидуального устройства идентификации или при подозрении о компрометации, личных ключей и паролей, а также при обнаружении нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к защищённой АРМ, несанкционированных (произведённых с

нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ, некорректного функционирования установленных на АРМ технических средств защиты, непредусмотренных отводов кабелей и подключённых устройств;

8) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закреплённого за ним АРМ, ставить в известность Администратора ИБ при необходимости внесения изменения в состав аппаратных и программных средств АРМ;

9) работать в ИС только в разрешённый период времени;

10) немедленно выполнять предписания Администратора ИБ и Администратора ИС, предоставлять им свой АРМ к анализу и работы с ним по их требованию;

11) ставить в известность Администратора ИС в случае появления сведений или подозрений о фактах несанкционированного доступа к информации, своей или чужой, а также отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т. п.), а также перебоев в системе электроснабжения;

12) осуществлять установленным порядком уничтожение информации, содержащей сведения конфиденциального характера с машинных носителей информации и из оперативной памяти АРМ;

13) уважать права других пользователей ИС на конфиденциальность и право пользования общими ресурсами;

14) сообщать своему непосредственному руководителю структурного подразделения (отдела) обо всех проблемах, связанных с эксплуатацией ИС и АРМ.

Пользователю категорически запрещается:

1) использовать компоненты программного и аппаратного обеспечения АРМ, в том числе и ИС в неслужебных целях;

2) самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств ИС (в том числе АРМ) или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формуляром на АРМ и (или) паспортом (техническим паспортом) на ИС;

3) осуществлять обработку информации, содержащей сведения конфиденциального характера, в присутствии посторонних (не допущенных к данной информации) лиц;

4) записывать и хранить конфиденциальную информацию на неучтённых носителях информации, в том числе для временного хранения;

5) оставлять включённое без присмотра АРМ, не активизировав временную блокировку экрана и клавиатуры (средствами защиты от НСД или операционных систем);

6) передавать кому-либо своё индивидуальное устройство идентификации (персональную ключевую дискету) в нарушение установленного порядка, делать неучтённые копии ключевого носителя, и вносить какие-либо изменения в файлы ключевого устройства идентификации;

7) оставлять без личного присмотра на рабочем месте или где бы то ни было свою персональную ключевую дискету, персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения конфиденциального характера);

8) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках ИС (в том числе средств защиты), которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность Администратора ИБ, Администратора ИС и руководителя своего структурного подразделения (отдела);

9) подбирать и отгадывать чужие пароли, а также собирать информацию о других пользователях ИС;

10) осуществлять попытки НСД к ресурсам системы и других пользователей ИС, проводить рассылку ложных, беспокоящих или угрожающих сообщений (писем);

11) фиксировать свои учётные данные (пароли, имена, идентификаторы, ключи) на материальных носителях;

12) разглашать ставшую известной в ходе выполнения своих обязанностей информацию, содержащую сведения конфиденциального характера;

13) вносить изменения в файлы, принадлежащие другим пользователям ИС.

4. Права пользователя

Пользователь ИС имеет право:

1) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закреплённого за ним АРМ;

2) участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;

3) своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных (функциональных) обязанностей;

4) требовать от Администратора ИБ и Администратора ИС смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

5. Правила работы в сетях общего доступа

Работа в сетях общего доступа и (или) международного обмена (сети Интернет) (далее – Сеть) на элементах ИС, должна производиться при служебной необходимости.

При работе в Сети запрещается:

1) осуществлять работу при отключённых средствах защиты (антивирусной защиты, средств от несанкционированного доступа и т. д.);

2) передавать по Сети защищаемую информацию без использования средств защиты каналов связи;

3) запрещается загружать из Сети программное обеспечение;

4) запрещается посещение сайтов сомнительной репутации (аморального содержания, содержащие нелегально распространяемое программное обеспечение или иной контент);

5) запрещается нецелевое использование подключения к Сети.

6. Ответственность

Пользователь ИС несёт персональную ответственность за:

1) ненадлежащее исполнение своих должностных (функциональных) обязанностей, а также сохранность комплекта АРМ, съёмных носителей информации, индивидуального средства идентификации и целостность установленного программного обеспечения;

2) разглашение сведений, отнесённых к сведениям конфиденциального характера, и сведений ограниченного распространения, ставших известными ему по роду работы.

Ответственность за нарушение функционирования ИС, уничтожение, блокирование, копирование, фальсификацию информации несёт пользователь ИС, под чьими идентификационными данными было совершено нарушение. Мера ответственности устанавливается по итогам служебного расследования.

Пользователи ИС, виновные в нарушениях, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством РФ и организационно-распорядительными документами Бюджетного учреждения.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

УТВЕРЖДЕНО

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО

**сотрудника государственного бюджетного учреждения
здравоохранения «Армавирский кожно-венерологический
диспансер» министерства здравоохранения Краснодарского
края, непосредственно осуществляющего обработку
персональных данных, в случае расторжения с ним трудового
договора прекратить обработку персональных данных,
ставших известными ему, в связи с исполнением
должностных обязанностей**

Я, _____, проживающий(-ая) по адресу
Ф.И.О.

_____, паспорт
серия _____, номер _____, выдан _____
«__» _____ года,

работая в должности _____
в государственном бюджетном учреждении здравоохранения «Армавирский
кожно-венерологический диспансер» министерства здравоохранения
Краснодарского края (далее – Бюджетное учреждение), в период настоящих
трудовых отношений и в течение 5 лет после их окончания, в соответствии с
Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О
персональных данных», обязуюсь:

1) не раскрывать третьим лицам и не распространять персональные
данные субъектов персональных данных Бюджетного учреждения, полученные
при исполнении мной должностных обязанностей;

2) при работе с персональными данными соблюдать требования,
описанные в «Правилах обработки персональных данных субъектов
персональных данных Бюджетного учреждения»;

3) выполнять относящиеся ко мне требования локальных нормативных
актов, касающихся обработки персональных данных;

4) в случае попытки посторонних лиц получить от меня персональные
данные субъектов персональных данных Бюджетного учреждения, сведения о
порядке обработки и защиты персональных данных, немедленно уведомить об
этом ответственного за организацию обработки персональных данных

Бюджетного учреждения и (или) руководителя своего структурного подразделения (отдела);

5) в случае расторжения со мною трудового договора, прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, и передать все носители персональных данных субъектов персональных данных – Бюджетного учреждения (документы, накопители данных в электронном виде, кино и фотонегативы и позитивы, и пр.) ответственному за организацию обработки персональных данных Бюджетного учреждения.

Я понимаю, что разглашение персональных данных субъектов персональных данных Бюджетного учреждения, может нанести ущерб субъектам персональных данных.

Я предупрежден(-а) о том, что, в случае разглашения или утраты мною сведений, относящихся к персональным данным субъектов персональных данных Бюджетного учреждения, я несу ответственность в соответствии со статьёй 90 Трудового Кодекса Российской Федерации и могу быть привлечен(-а) к материальной, гражданско-правовой, административной и уголовной ответственности в соответствии с действующим законодательством Российской Федерации.

Настоящим подтверждаю, что с «Правилами обработки персональных данных субъектов персональных данных Бюджетного учреждения» ознакомлен(-а).

« ____ » _____ 20 ____ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение 7

УТВЕРЖДЕНА

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ТИПОВАЯ ФОРМА
разъяснения субъекту персональных данных юридических
последствий отказа предоставить свои персональные данные

В соответствии с принципами обработки персональных данных, установленными Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», при обработке персональных данных должна быть обеспечена точность персональных данных, их достаточность, и актуальность по отношению к заявленной цели обработки персональных данных.

Кроме того, государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение) принимает необходимые меры по уточнению неполных или неточных персональных данных.

В случае, если субъект персональных данных отказывается предоставить свои персональные данные, либо представленные персональные данные являются неточными и (или) неполными по отношению к заявленной цели обработки персональных данных, Бюджетное учреждение оставляет за собой право отказать в предоставлении своих услуг субъекту персональных данных.

Если Бюджетное учреждение выявит факт умышленного представления субъектом неверных персональных данных, то Бюджетное учреждение может потребовать с субъекта персональных данных возмещения соответствующих затрат.

«___» _____ 20___ г.

(подпись)

(И.О. Фамилия)

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

ПОРЯДОК
доступа сотрудников государственного бюджетного
учреждения здравоохранения «Армавирский
кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края в помещения, в
которых ведётся обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных (далее – ПДн), средств вычислительной техники информационных систем, обрабатывающие ПДн, материальных носителей ПДн, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях.

Объектами охраны государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение) являются:

1) помещения, в которых происходит обработка ПДн как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

2) помещения, в которых хранятся материальные носители ПДн и резервные копии ПДн;

3) помещения, в которых установлены средства криптографической защиты информации (далее – СКЗИ), предназначенные для шифрования ПДн, в том числе носители ключевой информации (далее – спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются сотрудники Бюджетного учреждения, не допущенные к обработке ПДн и лица, не являющиеся сотрудниками Бюджетного учреждения.

К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут сотрудники структурных подразделений (отделов) Бюджетного учреждения, допущенные в помещения, являющиеся объектами охраны, а также их непосредственные руководители.

Контроль соблюдения требований, описанные в данном документе, обеспечивает должностное лицо, назначенный ответственным за организацию обработки ПДн в Бюджетном учреждении.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению. Например: металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведётся обработка ПДн, а также хранятся материальные носители ПДн и (или) их резервные копии, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа сотрудников Бюджетного учреждения, допущенных к обработке ПДн. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с ПДн. Например: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного или техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведётся обработка ПДн, лиц, из числа сотрудников Бюджетного учреждения, не допущенных к обработке ПДн.

В нерабочее время все окна и двери в помещениях (в том числе в смежных помещениях), в которых ведётся обработка ПДн, должны быть надёжно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы) или тумбочки, компьютеры выключены либо заблокированы.

Доступ сотрудников Бюджетного учреждения в помещения, в которых ведётся обработка ПДн в нерабочее время, в том числе в выходные и

праздничные дни, допускается только по письменному распоряжению и.о. главного врача, на основании предоставленных на его имя заявок (служебных записок) с перечнем сотрудников Бюджетного учреждения от руководителей структурных подразделений (отделов), доступ которым крайне необходим (с обоснованием, датой и временем выполняемых работ).

3. Правила доступа в серверные помещения

Доступ посторонних лиц в серверные помещения, в которых ведётся обработка ПДн, допускается по согласованию с ответственным за обеспечение безопасности информационных систем ПДн Бюджетного учреждения.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем ПДн Бюджетного учреждения.

Доступ сотрудников Бюджетного учреждения в серверные помещения в нерабочее время, в том числе в выходные и праздничные дни, допускается только по письменному распоряжению и.о. главного врача, на основании предоставленных на его имя заявок (служебных записок) с перечнем сотрудников Бюджетного учреждения от руководителей структурных подразделений (отделов), доступ которым крайне необходим (с обоснованием, датой и временем выполняемых работ).

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений и устройствами опечатывания в нерабочее время. Окна спецпомещений, расположенные на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или

охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами осуществляемых в помещении работ.

Для предотвращения просмотра спецпомещений извне, их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённый приказом и.о. главного врача.

Доступ иных лиц в спецпомещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц из числа сотрудников Бюджетного учреждения.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения (отдела) и (или) ответственного пользователя СКЗИ сотрудников Бюджетного учреждения.

При утрате ключа от входной двери в спецпомещение, необходимо заменить замок или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ сотрудников в спецпомещения в нерабочее время, в том числе в выходные и праздничные дни, допускается только по письменному распоряжению и.о. главного врача, на основании предоставленных на его имя заявок (служебных записок) с перечнем сотрудников Бюджетного учреждения

от руководителей структурных подразделений (отделов), доступ которым крайне необходим (с обоснованием, датой и временем выполняемых работ).

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

УТВЕРЖДЕНО

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ПОЛОЖЕНИЕ
по работе с инцидентами информационной безопасности в
государственном бюджетном учреждении здравоохранения
«Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края

1. Общие положения

Настоящее положение разработано в целях организации работы с инцидентами информационной безопасности в государственном бюджетном учреждении здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение).

Инцидент – одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее – ИС) и (или) к возникновению угроз безопасности информации, в том числе персональных данных.

Положение по работе с инцидентами информационной безопасности (далее – Положение) разработано в соответствии с:

- 1) Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- 2) Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- 3) требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;
- 4) требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18 февраля 2013 г. № 21;

5) требованиями по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждёнными приказом ФСТЭК России от 11 февраля 2013 г. № 17;

6) политикой обработки персональных данных субъектов Бюджетного учреждения.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.

Работа с инцидентами включает в себя следующие направления:

1) определение лиц, ответственных за выявление инцидентов и реагирование на них;

2) обнаружение, идентификация и регистрация инцидентов;

3) своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

4) анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

5) принятие мер по устранению последствий инцидентов;

6) планирование и принятие мер по предотвращению повторного возникновения инцидентов.

Для анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценки их последствий; планирования и принятия мер по предотвращению повторного возникновения инцидентов, назначается постоянно действующая комиссия по работе с инцидентами в соответствии с приказом и.о. главного врача.

2. Ответственные за выявление инцидентов и реагирование на них

2.1. В информационных системах.

Ответственными за выявление инцидентов в ИС являются:

1) лица, имеющие право доступа к ИС;

2) ответственный за техническое обслуживание ИС (администратор ИС);

3) ответственный за обеспечение безопасности в ИС (администратор ИБ).

Ответственными за реагирование на инциденты в ИС являются:

1) лица, имеющих право доступа к ИС;

2) руководитель подразделения (отдела) Бюджетного учреждения, в котором выявлен инцидент;

3) ответственный за техническое обслуживание ИС (администратор ИС);

4) ответственный за обеспечение безопасности в ИС (администратор ИБ);

5) ответственный за организацию обработки персональных данных Бюджетного учреждения, в случае, если ИС является информационной системой персональных данных и (или) государственной (муниципальной) информационной системой, обрабатывающей персональные данные;

6) председатель комиссии по работе с инцидентами.

2.2. Вне информационных систем.

Ответственными за выявление инцидентов вне ИС являются все сотрудники Бюджетного учреждения.

Ответственными за реагирование на инциденты вне ИС являются:

1) сотрудники Бюджетного учреждения, обнаружившие инцидент;

2) руководитель структурного подразделения (отдела) Бюджетного учреждения, в котором выявлен инцидент;

3) ответственный за организацию обработки персональных данных Бюджетного учреждения, в случае, если существует угроза безопасности персональных данных;

4) председатель комиссии по работе с инцидентами.

3. Обнаружение, идентификация и регистрация инцидентов

3.1. Работа по обнаружению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

1) выявление инцидентов в области информационной безопасности с помощью технических средств;

2) выявление инцидентов в области информационной безопасности в ходе контрольных мероприятий;

3) выявление инцидентов с помощью сотрудников Бюджетного учреждения.

3.2. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до сотрудников Бюджетного учреждения информации, позволяющей идентифицировать инциденты.

3.3. Регистрацию инцидентов осуществляет председатель комиссии по работе с инцидентами в журнале регистрации инцидентов информационной

безопасности. Рекомендуемая типовая форма журнала приведена в приложении к данному документу.

Хранение журнала должна осуществляться в местах, исключающих доступ к журналу посторонних лиц. Журнал хранится в течение 5 лет после завершения ведения. Ответственный за хранение журнала – председатель комиссии по работе с инцидентами.

4. Информирование о возникновении инцидентов

Сотрудник Бюджетного учреждения (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом сообщить об инциденте непосредственному своему руководителю структурного подразделения (отдела), администратору ИС, администратору ИБ, ответственному за организацию обработки персональных данных в Бюджетном учреждении, председателю комиссии по работе с инцидентами.

Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и даёт указания по дальнейшим действиям.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных (далее – ПДн), повлекшей нарушение прав субъекта(-ов) ПДн, председатель комиссии по работе с инцидентами уведомляет уполномоченный орган по защите прав субъектов ПДн:

1) в течение 24-х часов – о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет контактные сведения для взаимодействия с комиссией по инцидентам;

2) в течение 72-х часов – о результатах внутреннего расследования выявленного инцидента, а также сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5. Анализ инцидентов, а также оценка их последствий

Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценку их последствий осуществляет комиссия по работе с инцидентами информационной безопасности.

5.1. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:

- 1) действия организаций и отдельных лиц враждебные интересам Бюджетного учреждения;
- 2) отсутствие персональной ответственности сотрудников Бюджетного учреждения и их непосредственных руководителей за обеспечение информационной безопасности, в том числе персональных данных;
- 3) недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;
- 4) отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;
- 5) недостаточная техническая оснащённость структурного подразделения (отдела) или лица, ответственного за обеспечение информационной безопасности;
- 6) совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
- 7) наличие привилегированных бесконтрольных пользователей в информационной системе;
- 8) пренебрежение правилами и требованиями информационной безопасности сотрудниками Бюджетного учреждения;
- 9) и другие причины.

5.2. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.

6. Принятие мер по устранению последствий инцидентов

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

- 1) определение границ инцидента и ущерба от реализации угроз информационной безопасности;
- 2) ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.

7. Планирование и принятие мер по предотвращению инцидентов

7.1. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет комиссия по работе с инцидентами информационной безопасности и основывается на:

1) планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками Бюджетного учреждения;

2) проведении мероприятий по обучению сотрудников Бюджетного учреждения правилам и способам работы со средствами защиты информационных систем;

3) доведении до сотрудников норм законодательства, внутренних документов Бюджетного учреждения, устанавливающих ответственность за нарушение требований информационной безопасности;

4) разъяснительной работе с увольняющимися и принимаемыми на работу сотрудниками Бюджетного учреждения;

5) своевременной модернизации системы обеспечения информационной безопасности с учётом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;

6) своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.

7.2. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудников за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал Бюджетного учреждения является важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности могут являться основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение
к Положению по работе с
инцидентами информационной
безопасности в ГБУЗ Армавирском
КВД

Государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края

ЖУРНАЛ

регистрации инцидентов информационной безопасности государственного
бюджетного учреждения здравоохранения «Армавирский
кожно-венерологический диспансер» министерства здравоохранения
Краснодарского края

Начат «__» ____ 20__ года Окончен «__» ____ 20__ года

(должность)

(должность)

(подпись)

(И.О. Фамилия)

(подпись)

(И.О. Фамилия)

На ____ листах

[illegible]

Заместитель главного врача по
экономическим
вопросам экономической службы

О.В. Белоноскина

УТВЕРЖДЕНА

приказом ГБУЗ Армавирского КВД
от 25.06.2024 № 305-17

ИНСТРУКЦИЯ
по учёту, хранению и регистрации выдачи машинных
носителей персональных данных государственного
бюджетного учреждения здравоохранения «Армавирский
кожно-венерологический диспансер» министерства
здравоохранения Краснодарского края

1. Общие положения

Настоящая инструкция регламентирует порядок учёта, хранения и регистрации выдачи машинных носителей персональных данных государственного бюджетного учреждения здравоохранения «Армавирский кожно-венерологический диспансер» министерства здравоохранения Краснодарского края (далее – Бюджетное учреждение).

Настоящая инструкция разработана во исполнение требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Под машинными носителями в настоящей инструкции понимаются следующие носители информации:

- 1) дискеты;
- 2) оптические диски (CD, DVD) однократной и многократной записи;
- 3) электронные накопители информации (флэш-память, жесткие диски, в том числе и съёмные).

2. Термины и определения

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

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.

Персональные данные – любая информация, относящаяся к прямо или косвенно определённом или определяемому физическому лицу (субъекту персональных данных).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

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.

3. Порядок хранения и учёта машинных носителей

Машинные носители, содержащие персональные данные, подлежат обязательному учёту администратором информационной безопасности информационной системы. Учёт осуществляется с помощью «Журнала учёта носителей персональных данных». Рекомендуемая типовая форма журнала приведена в приложении к данному документу.

Носители, содержащие персональные данные, должны иметь специальную маркировку. Тип маркировки выбирается администратором информационной безопасности.

Съёмные носители должны храниться в сейфе или запираемом шкафу, расположенном в помещении Бюджетного учреждения, и изыматься только для выполнения должностных обязанностей.

В случае, если на съёмном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием средств криптографической защиты информации виде, допускается хранение таких носителей вне сейфов (запираемых шкафов).

При поступлении нового машинного носителя, который будет использоваться для хранения или передачи персональных данных,

администратор информационной безопасности регистрирует его в «Журнале учёта носителей персональных данных».

Машинные носители, которые не являются необходимыми для выполнения должностных обязанностей, хранятся в сейфе (запираемом шкафу) не более одного года, после чего их необходимо уничтожить без возможности восстановления с последующей регистрацией в «Журнале учёта носителей персональных данных».

4. Порядок регистрации выдачи машинных носителей

Учёт выдачи машинных носителей ведётся в «Журнале учёта носителей персональных данных», в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его роспись.

В случае возврата должностным лицом машинного носителя, в «Журнале учёта носителей персональных данных» администратором информационной безопасности проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

5. Ответственность

Персональную ответственность за соблюдение требований настоящей инструкции несёт администратор информационной безопасности Бюджетного учреждения.

За разглашение персональных данных и нарушение порядка обращения с машинными носителями, содержащими персональные данные, администратор информационной безопасности, а также лица, работающие с этими носителями, могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Заместитель главного врача по
экономическим
вопросам экономической службы



О.В. Белоноскина

Приложение
к Инструкции по учёту, хранению и
регистрации выдачи машинных
носителей ГБУЗ Армавирского
КВД

**Государственное учреждение здравоохранения «Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края**

ЖУРНАЛ
учёта носителей персональных данных

Начат «___» _____ 20__ года
Окончен «___» _____ 20__ года

(должность)

(должность)

/

1

(подпись)

(И.О. Фамилия)

(подпись)

(И.О. Фамилия)

На _____ листах

Приложение 11

УТВЕРЖДЕН

приказом ГБУЗ Армавирского КВД

Государственное бюджетное учреждение здравоохранения «Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края

ЖУРНАЛ

ознакомления сотрудников государственного бюджетного учреждения
здравоохранения «Армавирский кожно-венерологический диспансер»
министерства здравоохранения Краснодарского края, непосредственно
осуществляющих обработку персональных данных, с положениями
законодательства Российской Федерации о персональных данных (в том
числе с требованиями к защите персональных данных), локальными актами
по вопросам обработки персональных данных и (или) обучения указанных
сотрудников

Начат «__» _____ 20__ года Окончен «__» _____ 20__ года

(должность)

(должность)

(подпись)

(И.О. Фамилия)

(подпись)

(И.О. Фамилия)

На _____ листах

