

ПОЛИТИКА обработки и защиты персональных данных в БУЗОО «Клинический родильный дом № 6»

1. Общие положения

1.1 Настоящая Политика обработки и защиты персональных данных (далее Политика) бюджетного учреждения здравоохранения Омской области «Клинический родильный дом № 6» ИНН 5507045262, 644112, г. Омск, ул. Перелета, д.3 (далее - Оператор) разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом РФ, Гражданским кодексом Российской Федерации, Федеральными законами от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 года N 152-ФЗ "О персональных данных", Федеральным законом от 29.11.2010 г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 21.11.2011 №323-ФЗ «Об основах охраны здоровья граждан в РФ», Постановлением Правительства РФ от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказ Роскомнадзора от 24.02.2021 N 18 "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения", иными федеральными законами и нормативно-правовыми актами.

1.2 Политика разработана с целью реализации требований законодательства в области обработки и защиты персональных данных (ПДн) и направлена на обеспечение защиты прав и свобод субъекта персональных данных (ПДн) при обработке его ПДн Оператором, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Правовыми основаниями обработки ПДн является совокупность правовых актов, во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных.

Обработка ПДн в БУЗОО «КРД № 6» осуществляется в связи с выполнением учреждением функций, предусмотренных ее учредительными документами, действующим законодательством и определяемых:

- Федеральным законом от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";
- Федеральным законом от 27 июля 2006 года N 152-ФЗ "О персональных данных";
- Федеральным законом от 29.11.2010 г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;
- иными нормативно-правовыми актами РФ.

Кроме того, обработка ПДн Оператором осуществляется в ходе трудовых и иных, непосредственно связанных с ними отношений, в которых Оператор выступает в качестве работодателя (ТК РФ), в связи с реализацией Оператором своих прав и обязанностей как юридического лица,

также правовым основанием обработки ПДн является:

- договоры, заключаемые между оператором и субъектом персональных данных;
- согласие на обработку персональных данных.

2. Термины и определения.

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

2) 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;

3) Конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным сотрудников и пациентов, не допускать их распространения без согласия субъектов персональных данных или иного законного основания.

4) Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

5) Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

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

7) 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;

8) Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

9) Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

10) Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

11) Оператор - БУЗОО «КРД № 6» организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

12) Пациент - физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

13) Работники – лица, имеющие трудовые отношения с БУЗОО «КРД № 6», либо кандидаты на вакантную должность, вступившие с учреждением в отношения по поводу приема на работу.

14) Документы, содержащие персональные данные пациента - документы, необходимые для осуществления действий в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, а также для оформления договорных отношений.

15) Документы, содержащие персональные данные работника - документы, которые работник предоставляет Учреждению-оператору (работодателю) в связи с трудовыми отношениями и касающиеся конкретного работника (субъекта персональных данных), а также другие документы, содержащие сведения, предназначенные для использования в служебных целях.

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

17) Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

18) Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

19) Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

20) Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

21) Медицинская деятельность - профессиональная деятельность по оказанию медицинской помощи, проведению медицинских экспертиз, медицинских осмотров и медицинских освидетельствований, санитарно-противоэпидемических (профилактических) мероприятий и профессиональная деятельность, связанная с трансплантацией (пересадкой) органов и (или) тканей, обращением донорской крови и (или) ее компонентов в медицинских целях;

22) Лечащий врач - врач, на которого возложены функции по организации и непосредственному оказанию пациенту медицинской помощи в период наблюдения за ним и его лечения;

3. Принципы обеспечения безопасности персональных данных.

3.1. Основной задачей обеспечения безопасности ПДн при их обработке Оператором является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, уничтожения или искажения их в процессе обработки.

3.2. Обработка персональных данных пациентов и работников осуществляется на основе принципов:

- 1) Обработка персональных данных должна осуществляться на законной и справедливой основе, защита ПДн основывается на положениях нормативных актов и методических документов уполномоченных государственных органов.
- 2) Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- 3) Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- 4) Обработке подлежат только персональные данные, которые отвечают целям их обработки.
- 5) Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
- 6) При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждение-оператор должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- 7) Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен Федеральным законом № 152-ФЗ, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законодательством.
- 8) Вопрос о передаче БУЗОО «КРД № 6» своих персональных данных самостоятельно решает субъект персональных данных, так как он является собственником своих персональных данных.
- 9) Держателем персональных данных является БУЗОО «КРД № 6», которому субъект персональных данных добровольно передает во владение свои персональные данные. БУЗОО «КРД № 6» выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

10) Получение, хранение, комбинирование или любое другое использование персональных данных субъекта может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников и обучающихся, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.3. В учреждении не производится обработка ПДн несовместимая с целями их обработки.

3.4. При обработке ПДн обеспечивается их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Учреждение принимает необходимые меры по удалению или уничтожению неполных или неточных ПДн.

4. Перечень действий с персональными данными

При обработке ПДн оператор будет осуществлять следующие действия с ПДн: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

5. Обработка персональных данных.

5.1. Получение ПДн.

5.1.1. Все ПДн следует получать от самого субъекта. Если ПДн субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом или от него должно быть получено согласие.

5.1.2. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения ПДн, характере подлежащих получению ПДн, перечне действий с ПДн, сроке, в течение которого действует согласие, и порядке его отзыва, а также о последствиях отказа субъекта дать письменное согласие на их получению.

5.1.3. Документы, содержащие ПДн создаются путем:

- копирования оригиналов документов;
- внесение сведений в учетные формы;
- получение оригиналов необходимых документов.

5.1.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Оператором, определяется в соответствии с законодательством и локальными актами Оператора.

5.2. Обработка ПДн.

5.2.1. Обработка ПДн осуществляется в случаях, предусмотренных ст.ст.6, 10, 11 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", в том числе:

- с согласия субъекта ПДн на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона №152-ФЗ, при условии обязательного обезличивания персональных данных;
- в случаях, когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных, либо по его просьбе (персональные данные, сделанные общедоступными субъектом ПДн).

-обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

-обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

Доступ работников Оператора к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями законодательства, локальных актов учреждения.

Допущенные к обработке ПДн работники под роспись знакомятся с документами организации, устанавливающими порядок обработки ПДн.

5.2.2. Цели обработки персональных данных

- Обеспечение организации оказания медицинской помощи населению, а также наиболее полное исполнение обязательств и компетенций в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации", Федеральным законом от 29.11.2010 г. №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 12.04.2010 № 61-ФЗ "Об обращении лекарственных средств", Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства РФ от 04.10.2012 № 1006;

-Осуществление трудовых отношений;

- Осуществление гражданско-правовых отношений.

ПДн обрабатываются Оператором в следующих случаях:

- учет персональных данных пациентов и работников БУЗОО «КРД № 6».

-выполнение требований законодательства в сфере охраны здоровья граждан и обязательного медицинского страхования;

-выполнение требований законодательства в сфере труда и налогообложения;

-ведение текущего бухгалтерского и налогового учёта, формированию, изготовлению и своевременной подаче бухгалтерской, налоговой и статистической отчетности

- направления на прохождение ежегодного медицинского осмотра.

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством, в частности:

-индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и обязательного медицинского страхования;

-сбор, обработка и передача данных в регистр медицинских и фармацевтических работников;

-сбор, обработка и передача данных в регистр оплаты услуг по линии обязательного медицинского страхования;

-обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

-обработка персональных данных необходима для информационного обеспечения Оператора и субъектов персональных данных.

-обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, разрешенные субъектом персональных данных для распространения), включая размещение на официальном сайте.

5.2.3. Категории субъектов ПДн

В БУЗОО «КРД № 6» обрабатываются ПДн следующих субъектов:

- физические лица, состоящие в с учреждением в трудовых правоотношениях;
- физические лица, являющиеся близкими родственниками сотрудников учреждения;
- физические лица, уволившиеся из учреждения;
- физические лица-кандидаты на трудоустройство;
- физические лица, состоящие с учреждением в гражданско-правовых отношениях;
- физические лица, обратившиеся в учреждение за оказанием медицинской помощи.

Основанием для обработки ПДн субъекта, не являющегося работником Оператора или лицом, заключившим с Оператором договор, является согласие в письменной форме субъекта персональных данных на обработку его ПДн или добровольное размещение непосредственно субъектом ПДн своих персональных данных в общедоступных источниках информации.

Субъект персональных данных принимает решение о предоставлении его ПДн и дает согласие на их обработку свободно, своей волей и в своем интересе.

Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям обработки.

Полный перечень ПДн представлен в Положении об обработке персональных данных в БУЗОО «КРД № 6», утвержденным руководителем организации.

5.2.4. Обработка ПДн ведется:

- ПДн работников обрабатываются с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, и без использования таких средств, с фиксацией ПДн на материальном носителе (бумажные документы).
- ПДн лиц, которым оказываются медицинские и медико-социальные услуги обрабатываются Оператором с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, без использования таких средств, с фиксацией ПДн на материальном носителе (бумажные документы).

5.3. Персональные данные, разрешенные субъектом персональных данных для распространения.

5.3.1. Персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;

5.3.2. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных статьей 10.1 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

5.3.3. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных., при этом его содержание должно соответствовать требованиям, установленным уполномоченным органом по защите прав субъектов персональных данных.

5.3.4. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

В случае, если из предоставленного субъектом персональных данных согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, не следует, что субъект персональных данных не установил запреты и условия на обработку персональных данных, предусмотренные ч.9.ст.10.1. Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", или если в предоставленном субъектом персональных

данных таком согласии не указаны категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты в соответствии с частью 9 ст.10.1 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", такие персональные данные обрабатываются оператором, которому они предоставлены субъектом персональных данных, без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с персональными данными неограниченному кругу лиц.

5.3.5.Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору: - непосредственно;
- с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

5.3.6. Молчание или бездействие субъекта персональных данных ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

5.3.7. В согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения, субъект персональных данных вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных оператором неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц. Отказ оператора в установлении субъектом персональных данных запретов и условий, предусмотренных настоящей статьёй, не допускается.

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

5.3.9. Действие согласия субъекта персональных данных на обработку персональных данных, разрешенных субъектом персональных данных для распространения, прекращается с момента поступления оператору требования, о прекращении передачи персональных данных, разрешенных субъектом персональных данных для распространения.

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

5.4. Хранение ПДн

5.4.1.ПДн субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

5.4.2.ПДн, зафиксированные на бумажных носителях, хранятся в запираемых шкафах (сейфах), либо в запираемых помещениях с ограниченным правом доступа..

5.4.3. ПДн субъектов, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (вкладках).

5.4.4. Хранение ПДн в форме, позволяющей определить субъекта ПДн, осуществляется не дольше, чем этого требуют цели их обработки.

5.5. Уничтожение ПДн

5.5.1. Условия и сроки уничтожения персональных данных Оператором:

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель – в срок, не превышающий 30 дней с даты достижения целей обработки ПДн, если иное не предусмотрено законом.;

- достижение максимальных сроков хранения документов, содержащих персональные данные, – в течение 30 дней с наступления окончания срока хранения;

-предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в срок, не превышающий семи рабочих дней;

- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

5.5.2. При достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- Оператор не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

5.5.3. Уничтожение персональных данных осуществляет комиссия, созданная приказом руководителя учреждения.

5.5.4. Факт уничтожения ПДн подтверждается документально актом об уничтожении носителей, составленным в соответствии с требованиями, установленными Приказом Роскомнадзора №179 от 28.10.2022 г «Об утверждении Требований к подтверждению уничтожения персональных данных», подписанным членами комиссии.

5.6. Передача ПДн.

5.6.1. Организация передает ПДн третьим лицам в следующих случаях:

- субъект выразил свое согласие на такие действия;

- передача предусмотрена российским или иным применимым законодательством в рамках установленной законодательством процедуры.

5.6.2. Перечень третьих лиц, которым передаются ПД.

Пенсионный фонд РФ для учета (на законных основаниях);

Налоговые органы РФ (на законных основаниях);

Фонд социального страхования (на законных основаниях);

Территориальный фонд обязательного медицинского страхования (на законных основаниях);

Страховые медицинские организации по обязательному и добровольному медицинскому страхованию (на законных основаниях);

Банки для начисления заработной платы (на основании договора);

Судебные и правоохранительные органы, в случаях, установленных законодательством.

Органы ЗАГС, в случаях, установленных законодательством.

-иные органы и организации, в случаях, предусмотренных законодательством.

6. Обеспечение защиты персональных данных при их обработке Оператором

6.1. Оператор принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июня 2006 № 152 - ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27 июня 2006 № 152 - ФЗ «О персональных данных», Постановлением Правительства от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами.

6.2. Оператор принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, распространения и других несанкционированных действий, в том числе:

-определяет угрозы безопасности персональных данных при их обработке;

- принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;
- назначает лиц, ответственных за обеспечение безопасности персональных данных в структурных подразделениях и информационных системах Оператора;
- создает необходимые условия для работы с персональными данными;
- организует учет документов, содержащих персональные данные;
- организует работу с информационными системами, в которых обрабатываются персональные данные;
- хранит персональные данные в условиях, при которых обеспечивается их сохранность и исключается неправомерный доступ к ним;

6.3. В соответствии с требованиями нормативных документов Оператором создана система защиты ПДн (СЗПДн), состоящая из подсистем правовой, организационной и технической защиты.

6.4. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПДн.

6.5. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнерами и сторонними лицами, защиты информации в открытой печати, рекламной и публикаторской деятельности, аналитической работы.

6.6. Подсистема технической защиты включает комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту ПДн.

6.7. Основными мерами защиты ПДн Оператора являются:

- 6.7.1. назначение Оператором ответственного за организацию обработки персональных данных;
- 6.7.2. издание Оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- 6.7.3. применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- 6.7.4. осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Оператора в отношении обработки персональных данных, локальным актам оператора;
- 6.7.5. оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- 6.7.6. ознакомление работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.
- 6.7.8. Определение актуальных угроз безопасности ПДн при их обработке в ИСПД и разработке мер и мероприятий по защите ПДн.
- 6.7.9. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

6.7.8. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления персональных данных, а также от иных неправомерных действий в отношении персональных данных.

6.7.9. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

- в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемом вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;

- в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

7. Права и обязанности субъекта персональных данных и Оператора персональных данных.

7.1. Субъект ПДн вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.2. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

7.3. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

7.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Оператором;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Оператором способы обработки персональных данных;
- наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу.

7.5. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.6. Субъект персональных данных имеет право требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения, в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

7.7. Оператор ПДн обязан:

7.7.1. При сборе персональных данных предоставлять информацию по их обработке;

7.7.2. При отказе от предоставления ПДн субъекту разъясняются последствия такого отказа;

7.7.3. Опубликовать или иным способом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях по защите ПДн;

7.7.4. Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

7.7.5. Давать ответы на запросы и обращения субъектов ПДн, их представителей и уполномоченного органа по защите прав субъектов ПДн.

8. Актуализация, исправление, удаление, уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

8.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки персональных данных, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются Оператором субъекту персональных данных или его представителю в течение 10 рабочих дней с момента обращения либо получения запроса субъекта персональных данных или его представителя. Данный срок может быть продлен, но не более чем на пять рабочих дней. Для этого Оператору следует направить субъекту персональных данных мотивированное уведомление с указанием причин продления срока предоставления запрашиваемой информации.

8.2. В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

8.3. Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

- подпись субъекта персональных данных или его представителя.

8.4. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.5. Оператор предоставляет сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

8.6. Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Закона о персональных данных все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

8.7. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

8.8. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

8.9. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо Роскомнадзором, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

8.10. В случае выявления неправомерной обработки персональных данных при обращении (запросе) субъекта персональных данных или его представителя либо Роскомнадзора Оператор осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения запроса.

8.11. При выявлении Оператором, Роскомнадзором или иным заинтересованным лицом факта неправомерной или случайной передачи (предоставления, распространения) персональных данных (доступа к персональным данным), повлекшей нарушение прав субъектов персональных данных, Оператор:

- в течение 24 часов - уведомляет Роскомнадзор о произошедшем инциденте, предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, предполагаемой вреде, нанесенном правам субъектов персональных данных, и принятых мерах по устранению последствий инцидента, а также предоставляет сведения о лице, уполномоченном Оператором на взаимодействие с Роскомнадзором по вопросам, связанным с инцидентом;

- в течение 72 часов - уведомляет Роскомнадзор о результатах внутреннего расследования выявленного инцидента и предоставляет сведения о лицах, действия которых стали его причиной (при наличии).

8.12. Порядок уничтожения персональных данных Оператором.

8.13. Условия и сроки уничтожения персональных данных Оператором:

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;

- достижение максимальных сроков хранения документов, содержащих персональные данные, - в течение 30 дней;

- предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в течение семи рабочих дней;

- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не требуется, - в течение 30 дней.

8.14. При достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- Оператор вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

- иное не предусмотрено другим соглашением между Оператором и субъектом персональных данных.

8.15. Уничтожение персональных данных осуществляется в соответствии с требованиями действующего законодательства, комиссией, созданной приказом руководителя «БУЗОО «КРД № 6».

9. Заключительные положения

9.1. Настоящая Политика утверждается и вводится в действие распорядительным документом, подписываемым руководителем Оператора.

9.2. В настоящую Политику могут вноситься изменения и дополнения, утверждаемые приказом руководителя Оператора.

9.3. Электронная версия Политики размещается на официальном сайте учреждения.