

УТВЕРЖДЕНО

приказом от 18.11.2024 г. № 539/1-Д

**Положение об обработке персональных данных
в Санкт-Петербургском государственном бюджетном учреждении здравоохранения
«Городская поликлиника № 71»**

Оглавление

1. Основные понятия	3
2. Общие положения	6
3. Цели, правовые основания обработки персональных данных, категории субъектов персональных данных, перечень действий с персональными данными	8
3.1. Участие в трудовых взаимоотношениях с работниками.....	8
3.2. Обеспечение соблюдения законодательства в сфере здравоохранения	10
4. Принципы и условия обработки персональных данных	12
5. Права субъектов персональных данных.....	19
6. Обязанности Учреждения и меры, направленные на обеспечение их выполнения	23

1. Основные понятия

В настоящем Положении используются следующие основные понятия:

- автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;
- блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- врачебная тайна – сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении;
- документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель;
- информация – сведения (сообщения, данные) независимо от формы их представления;
- 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 выполнения оператором и иными лицами, получившими доступ к персональным данным, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;
- машинный носитель информации – любое техническое устройство, предназначенное для фиксации, хранения, накопления, преобразования и передачи информации (флеш-накопитель, оптический диск, карта памяти, жесткий диск и т.д.);
- 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;
- 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;

— 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;

— пациент – физическое лицо, которому оказывается медицинская помощь или которое обратилось за оказанием медицинской помощи независимо от наличия у него заболевания и от его состояния;

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

— 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 законом о персональных данных;

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

— работник – физическое лицо, вступившее в трудовые отношения с работодателем;

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

— сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет";

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

— 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;

— угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

— электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

2. Общие положения

2.1. Настоящее Положение (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. N 152-ФЗ «О персональных данных», принятыми в соответствии с ними подзаконными актами и иными нормативно-правовыми актами в области персональных данных (далее – законодательство).

2.2. Положение определяет правила и порядок обработки персональных данных, устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства, а также определяет для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в Санкт-Петербургском государственном бюджетном учреждении здравоохранения «Городская поликлиника № 71» (далее – Учреждение).

2.3. Положение распространяется на все отношения, связанные с обработкой персональных данных субъектов персональных данных, осуществляемой Учреждением с использованием средств автоматизации (автоматизированная обработка персональных данных) и без использования средств автоматизации.

2.4. Порядок ввода в действие и изменения Положения.

2.4.1. Положение вступает в силу с момента его утверждения Приказом главного врача Учреждения и действует до утверждения новой редакции Положения или до его отмены.

2.4.2. Положение подлежит пересмотру в ходе периодического анализа ответственного за организацию обработки персональных данных в Учреждении, при изменении процессов обработки персональных данных, а также в случаях изменения законодательства.

2.4.3. Все изменения в Положение вносятся Приказом главного врача Учреждения.

2.5. Положение подлежит опубликованию на официальном сайте в сети «Интернет» Учреждения.

2.6. С Положением должны быть ознакомлены все работники Учреждения под подпись.

2.7. Работники Учреждения, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных (соблюдать конфиденциальность персональных данных), если иное не предусмотрено законом о персональных данных.

2.8. Работники Учреждения, непосредственно связанные с обработкой или защитой персональных данных, а также ответственный за организацию обработки персональных данных также должны быть ознакомлены под подпись с Положением и руководствоваться им.

3. Цели, правовые основания обработки персональных данных, категории субъектов персональных данных, перечень действий с персональными данными

3.1. Участие в трудовых взаимоотношениях с работниками

3.1.1. Цель обработки персональных данных: участие в трудовых взаимоотношениях с работниками, в том числе:

- заключение и исполнение обязательств по трудовым договорам;
- осуществление кадрового, бухгалтерского и воинского учета;
- получение образования работниками и повышение квалификации работников;
- проведение специальной оценки условий труда работников;
- обеспечение личной безопасности работников;
- контроль количества и качества выполняемой работы;
- обеспечение сохранности имущества;
- внесение информации о медицинском работнике в медицинскую информационную систему и федеральный регистр медицинских работников;
- распространение информации о медицинских работниках на сайте в сети «Интернет» Учреждения;
- распространение контактных данных на сайте в сети «Интернет» Учреждения;
- размещение информации о работниках (в том числе контактных данных) на информационных ресурсах Учреждения;
- иные действия, не противоречащие законодательству и непосредственно связанные с организацией эффективной работы Учреждения.

3.1.2. Правовыми основаниями для указанной цели являются:

- Трудовой кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Федеральный закон от 06.12.2011 г. N 402-ФЗ «О бухгалтерском учете»;
- Федеральный закон от 28.03.1998 г. N 53-ФЗ «О воинской обязанности и военной службе»;
- Федеральный закон от 21.11.2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 29.12.2006 г. N 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;

— Федеральный закон от 01.04.2006 г. N 27-ФЗ «Об индивидуальном (персонифицированном) учете в системах обязательного пенсионного страхования и обязательного социального страхования»;

— Федеральный закон от 28.12.2013 г. N 426-ФЗ «О специальной оценке условий труда»;

— Федеральный закон от 16.07.1999 г. N 165-ФЗ «Об основах обязательного социального страхования»;

— Федеральный закон от 15.12.2001 г. N 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

— Федеральный закон от 24.07.1996 г. N 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»;

— Федеральный закон от 30.03.1999 г. N 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»;

— Федеральный закон от 24.11.1995 г. N 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

— Федеральный закон от 27.07.2006 г. N 152-ФЗ «О персональных данных».

3.1.3. Категория субъектов, персональные данные которых обрабатываются: работники и бывшие работники Учреждения, их родственники.

3.1.4. Категории обрабатываемых персональных данных для достижения указанной цели:

— фамилия, имя и отчество (при наличии);

— дата и место рождения;

— пол;

— гражданство;

— вид, серия, номер основного документа, удостоверяющего личность; наименование органа, выдавшего данный документ; дата выдачи;

— идентификационный номер налогоплательщика;

— страховой номер индивидуального лицевого счета;

— реквизиты банковского счета;

— адрес регистрации места жительства, дата регистрации по месту жительства;

— адрес фактического проживания;

— сведения о воинском учете, в том числе отношение к воинской обязанности;

— сведения о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовых функций;

- сведения об образовании, повышении квалификации или о наличии специальных знаний;
- сведения о трудовой деятельности, в том числе информация о предыдущих местах работы, периодах и стаже работы;
- сведения о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о его прекращении;
- сведения о семейном положении, составе семьи (степень родства, фамилии, имена, отчества (при наличии), даты рождения);
- сведения, содержащиеся в приказах по личному составу;
- номер контактного телефона;
- адрес электронной почты;
- фотография;
- сведения о доходах;
- социальное положение;
- иные персональные данные, которые работник пожелал сообщить, и обработка которых соответствует цели обработки.

3.2. Обеспечение соблюдения законодательства в сфере здравоохранения

3.2.1. Цель обработки персональных данных: обеспечение соблюдения законодательства в сфере здравоохранения, в том числе:

- оказание медицинских услуг;
- установление медицинского диагноза;
- оформление медицинской, отчетной и статистической документации, направлений на обследования, лечебные процедуры, консультации специалистов;
- ведение электронной медицинской карты пациента;
- рассмотрение обращений пациентов;
- иные действия, не противоречащие законодательству и непосредственно связанные с процессом оказания квалифицированной медицинской помощи.

3.2.2. Правовыми основаниями для указанной цели являются:

- Федеральный закон от 21.11.2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральный закон от 29.11.2010 г. N 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

— Федеральный закон от 27.07.2006 г. N 152-ФЗ «О персональных данных».

3.2.3. Категория субъектов, персональные данные которых обрабатываются: пациенты Учреждения.

3.2.4. Категории обрабатываемых персональных данных для достижения указанной цели:

- фамилия, имя и отчество (при наличии);
- дата и место рождения;
- пол;
- гражданство;
- вид, серия, номер основного документа, удостоверяющего личность; наименование органа, выдавшего данный документ; дата выдачи;
- страховой номер индивидуального лицевого счета;
- номер полиса обязательного медицинского страхования застрахованного лица (при наличии);
- анамнез, диагноз, вид, сроки, объем и условия оказания медицинской помощи;
- результат обращения за медицинской помощью;
- серия и номер выданного листка нетрудоспособности (при наличии);
- сведения об оказанных медицинских услугах;
- примененные стандарты медицинской помощи;
- сведения об организации, оказавшей медицинские услуги.

3.2.5. Перечень действий с персональными данными: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), блокирование, удаление, уничтожение.

4. Принципы и условия обработки персональных данных

4.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных законодательством.

4.2. Обработка персональных данных осуществляется на основе принципов:

4.2.1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

4.2.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

4.2.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4.2.4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

4.2.5. 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.

4.2.6. 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 должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

4.2.7. 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 законом о персональных данных, 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 законом о персональных данных.

4.3. Обработка персональных данных допускается в следующих случаях:

4.3.1. обработка персональных данных осуществляется с согласия субъекта персональных данных (или его законного представителя) на обработку персональных данных в соответствии с п. 1 ч. 1 ст. 6, ч. 1 ст. 8, п. 1 ч. 2 ст. 10, ч. 1 ст. 10.1 и ч. 1 ст. 11 закона о персональных данных;

4.3.2. обработка персональных данных осуществляется без согласия субъекта персональных данных в случаях, предусмотренных п. 2–11 ч. 1 ст. 6, п. 2–10 ч. 2 ст. 10 и ч. 2 ст. 11 закона о персональных данных, а также ч. 3–5 ст. 6 закона о персональных данных, когда Учреждение обрабатывает персональные данные по поручению иного оператора.

4.4. Обработка персональных данных осуществляется без согласия субъектов персональных данных в следующих случаях:

4.4.1. 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. Заключаемый с субъектом персональных данных договор не может содержать положения, ограничивающие права и свободы субъекта персональных данных, устанавливающие случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положения, допускающие в качестве условия заключения договора бездействие субъекта персональных данных.

4.4.2. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

4.4.3. 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.

4.4.4. Обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

4.4.5. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.4.6. Обработка персональных данных осуществляется по поручению иного оператора персональных данных. В соответствии с ч. 3 ст. 6 закона о персональных данных иной оператор вправе поручить обработку персональных данных Учреждению с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с Учреждением договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным

органом соответствующего акта (далее – поручение оператора). Учреждение, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных законом о персональных данных. В поручении оператора должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться Учреждением, цели их обработки, должна быть установлена обязанность Учреждения соблюдать конфиденциальность персональных данных, требования, предусмотренные ч. 5 ст. 18 и ст. 18.1 закона о персональных данных, обязанность по запросу оператора персональных данных в течение срока действия поручения оператора, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения оператора требований, установленных в соответствии со ст. 6 закона о персональных данных, обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 закона о персональных данных, в том числе требование об уведомлении оператора о случаях, предусмотренных ч. 3.1 ст. 21 закона о персональных данных. В соответствии с ч. 4 ст. 6 закона о персональных данных Учреждение, осуществляющее обработку персональных данных по поручению иного оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В соответствии с ч. 5 ст. 6 закона о персональных данных в случае если иной оператор поручает обработку персональных данных Учреждению, ответственность перед субъектом персональных данных за действия Учреждения несет оператор. Учреждение, осуществляющее обработку персональных данных по поручению иного оператора, несет ответственность перед оператором.

4.5. Обработка сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются для установления личности субъекта персональных данных, Учреждением не осуществляется.

4.6. Трансграничная передача персональных данных Учреждением не осуществляется.

4.7. Передача персональных данных возможна при наличии письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях

предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных действующим законодательством Российской Федерации.

4.8. Учреждение получает все персональные данные работника у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник уведомляется об этом заранее, Учреждение получает от него письменное согласие. Учреждение сообщает работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.9. Учреждение не обрабатывает информацию (персональные данные) работников об их членстве в общественных объединениях или их профсоюзной деятельности за исключением случаев, предусмотренных Трудовым кодексом или иными федеральными законами.

4.10. Учреждение вправе поручить обработку персональных данных иному оператору с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим оператором договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта. Оператор, которому Учреждение предполагает поручить обработку персональных данных, должен быть зарегистрирован в реестре операторов уполномоченного органа по защите прав субъектов персональных данных. Оператор, осуществляющий обработку персональных данных по поручению Учреждения, обязан соблюдать принципы и правила обработки персональных данных, предусмотренные законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных законом о персональных данных. В поручении Учреждения должны быть определены перечень персональных данных, перечень действий (операций) с персональными данными, которые будут совершаться оператором, цели их обработки, должна быть установлена обязанность оператора соблюдать конфиденциальность персональных данных, требования, предусмотренные ч. 5 ст. 18 и ст. 18.1 закона о персональных данных, обязанность по запросу Учреждения в течение срока действия поручения Учреждения, в том числе до обработки персональных данных, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Учреждения требований, установленных в соответствии со ст. 6 закона о персональных данных,

обязанность обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 закона о персональных данных, в том числе требование об уведомлении Учреждения о случаях, предусмотренных ч. 3.1 ст. 21 закона о персональных данных. Оператор, осуществляющий обработку персональных данных по поручению Учреждения, не обязан получать согласие субъекта персональных данных на обработку его персональных данных. В случае если Учреждение поручает обработку персональных данных иному оператору, ответственность перед субъектом персональных данных за действия оператора несет Учреждение. Оператор, осуществляющий обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

4.11. Обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется в Учреждении с соблюдением запретов и условий, предусмотренных ст. 10.1 закона о персональных данных.

4.12. Сроки обработки персональных данных определяются в соответствии с законодательством Российской Федерации.

4.13. Сбор персональных данных осуществляется в пределах установленного объема, необходимого для каждой категории субъектов персональных данных, с которыми взаимодействует Учреждение, и не может превышать указанный объем.

4.14. Условием прекращения обработки персональных данных может являться достижение целей их обработки, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных, если иное не предусмотрено законом о персональных данных.

4.15. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным, то есть содержать информацию, позволяющую однозначно сделать вывод о целях, способах обработки с указанием действий, совершаемых с персональными данными, объёме обрабатываемых персональных данных. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Учреждением. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных, при этом в случае отзыва Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных в случаях, определённых ч. 2 ст. 9 закона о персональных данных.

4.16. Любое согласие субъекта персональных данных (в том числе согласие на обработку, на предоставление персональных данных в адрес третьих лиц, на трансграничную передачу, на распространение) является правом субъекта, а не обязанностью. Ни один из субъектов персональных данных не обязан давать никакое своё согласие без своего желания. В случае если согласие субъекта персональных данных не требуется, обработка персональных данных осуществляется в Учреждении без согласия субъекта персональных данных. В ином случае если согласие субъекта персональных данных требуется, но субъект персональных данных отказывается давать такое согласие, любые последующие действия или услуги, порождаемые таким согласием, Учреждением не осуществляются (не оказываются). Во всех случаях наличие или отсутствие согласия субъекта персональных данных не отменяет обязательность соблюдения требований конфиденциальности персональных данных (за исключением общедоступной информации).

4.17. В случаях, когда требуется согласие субъекта персональных данных, оно даётся в письменной форме, за исключением согласия в формате электронного документа. В соответствии со ст. 6 Федерального закона от 06.04.2011 г. N 63-ФЗ «Об электронной подписи» равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в виде электронного документа, подписанного УКЭП. Согласие в виде электронного документа, подписанного УКЭП, может быть получено от субъекта персональных данных по электронной почте, при этом электронная подпись к такому согласию подлежит немедленной проверке получателем в порядке, установленном в документации на средство электронной подписи. Получатель проверяет действительность УКЭП субъекта и при положительном результате проверки факт подписания согласия считается подтвержденным. После успешной проверки получатель обязан принять необходимые немедленные меры для обеспечения хранения согласия субъекта персональных данных в виде электронного документа, подписанного УКЭП. Скриншот результата успешной проверки должен быть сохранён получателем в виде электронного документа, подписанного УКЭП получателя, вместе с согласием субъекта персональных данных в виде электронного документа, подписанного УКЭП. Независимо от результатов проверки согласие подлежит уничтожению из электронной почты. Запрещается вывод на печать и пересылка по электронной почте согласий, полученных в виде электронных документов, подписанных УКЭП. Согласие субъекта персональных данных на обработку его персональных данных в письменной форме должно включать в себя, в частности:

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

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

— наименование и адрес Учреждения, получающего согласие субъекта персональных данных;

— цель обработки персональных данных;

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

— наименование или фамилию, имя, отчество (при его наличии) и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка будет поручена такому лицу;

— перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;

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

— подпись субъекта персональных данных и дата оформления согласия.

4.18. Согласия на обработку персональных данных в письменной форме обрабатываются исключительно неавтоматизированным способом – в бумажном виде. Сканирование таких согласий и их последующая обработка в электронном виде запрещаются. В случае получения скана таких согласий от субъектов персональных данных по электронной почте запрещается их вывод на печать, а также сохранение в виде файлов и пересылка по электронной почте, такие согласия подлежат немедленному уничтожению из электронной почты.

5. Права субъектов персональных данных

5.1. Право субъекта персональных данных на доступ к его персональным данным

5.1.1. Субъект персональных данных имеет право на получение информации (далее – запрашиваемая субъектом информация), касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Учреждением;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Учреждением способы обработки персональных данных;
- наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании закона о персональных данных;
- 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 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 Учреждения, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Учреждением обязанностей, установленных ст. 18.1 закона о персональных данных;
- иные сведения, предусмотренные законодательством.

5.1.2. Субъект персональных данных имеет право на получение запрашиваемой субъектом информации, за исключением следующих случаев:

- обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

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

— обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

— доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

5.1.3. Субъект персональных данных вправе требовать от Учреждения 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.

5.1.4. Запрашиваемая субъектом информация должна быть предоставлена субъекту персональных данных Учреждением в доступной форме, и в ней не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

5.1.5. Запрашиваемая информация предоставляется субъекту персональных данных или его представителю Учреждением в течение десяти рабочих дней с момента обращения либо получения Учреждением запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Учреждением в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. 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 Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения) либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением; подпись субъекта персональных данных или его представителя

(далее – необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан УКЭП в соответствии с законодательством Российской Федерации. Учреждение предоставляет запрашиваемые сведения субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение или запрос, если иное не указано в обращении или запросе.

5.1.6. В случае если запрашиваемая субъектом информация, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения запрашиваемой субъектом информации и ознакомления с такими персональными данными не ранее чем через тридцать дней (далее – нормированный срок запроса) после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законом о персональных данных, принятым в соответствии с ним нормативно-правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5.1.7. Субъект персональных данных вправе обратиться повторно в Учреждение или направить повторный запрос в целях получения запрашиваемой субъектом информации, а также в целях ознакомления с обрабатываемыми персональными данными, до истечения нормированного срока запроса в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимой для запроса информацией должен содержать обоснование направления повторного запроса.

5.1.8. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса возлагается на Учреждение.

5.2. Право субъекта персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

5.2.1. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении

субъекта персональных данных или иным образом затрагивающих его права и законные интересы, Учреждением не осуществляется.

5.3. Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации

5.3.1. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации, Учреждением не осуществляется.

5.4. Право на обжалование действий или бездействия Учреждения

5.4.1. Если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований закона о персональных данных или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Учреждения в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

5.5. Право на отзыв согласия на обработку персональных данных

5.5.1. Субъект персональных данных имеет право на отзыв согласия на обработку персональных данных, данного Учреждению.

6. Обязанности Учреждения и меры, направленные на обеспечение их выполнения

6.1. Обязанности Учреждения при сборе персональных данных

6.1.1. При сборе персональных данных Учреждение предоставляет субъекту персональных данных по его просьбе запрашиваемую информацию, касающуюся обработки его персональных данных в соответствии с ч. 7 ст. 14 закона о персональных данных.

6.1.2. Если в соответствии с законом о персональных данных предоставление персональных данных и (или) получение Учреждением согласия на обработку персональных данных являются обязательными, Учреждение разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные и (или) дать согласие на их обработку.

6.1.3. Если персональные данные получены не от субъекта персональных данных, Учреждение до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию (далее – информация, сообщаемая при получении персональных данных не от субъекта персональных данных):

- наименование и адрес Учреждения или представителя Учреждения;
- цель обработки персональных данных и ее правовое основание;
- перечень персональных данных;
- предполагаемые пользователи персональных данных;
- установленные законом о персональных данных права субъекта персональных данных;
- источник получения персональных данных.

6.1.4. Учреждение не предоставляет субъекту информацию, сообщаемую при получении персональных данных не от субъекта персональных данных, в случаях, если:

- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Учреждением;
- персональные данные получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
- обработка персональных данных, разрешенных субъектом персональных данных для распространения, осуществляется с соблюдением запретов и условий, предусмотренных ст. 10.1 закона о персональных данных;

— предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

6.1.5. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», Учреждение обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации, обрабатываемых в информационных системах с использованием баз данных, находящихся на территории Российской Федерации.

6.2. Обязанности Учреждения при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

6.2.1. Учреждение сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Учреждения в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Учреждение дает в письменной форме мотивированный ответ в срок, не превышающий десяти рабочих дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Учреждением в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.2.3. Учреждение предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися

к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение уничтожает такие персональные данные. Учреждение уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

6.2.4. Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Учреждением в адрес уполномоченного органа по защите прав субъектов персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.3. Обязанности Учреждения по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных

6.3.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных, Учреждение осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их

блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) 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.

6.3.2. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.3.3. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.3.4. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Учреждение с момента выявления такого инцидента Учреждением, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

— в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также о лице,

уполномоченном в Учреждении для взаимодействия с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

— в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также о лицах, действия которых стали причиной выявленного инцидента (при наличии).

6.3.5. В случае достижения цели обработки персональных данных Учреждение прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законом о персональных данных или другими федеральными законами.

6.3.6. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законом о персональных данных или другими федеральными законами.

6.3.7. В случае обращения субъекта персональных данных с требованием о прекращении обработки персональных данных Учреждение в срок, не превышающий десяти рабочих дней с даты получения соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка

осуществляется лицом, осуществляющим обработку персональных данных, действующим по поручению Учреждения), за исключением случаев, предусмотренных п. 2-11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 закона о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления Учреждением в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

6.3.8. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Учреждение блокирует такие персональные данные или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.4. Меры, направленные на обеспечение выполнения обязанностей, предусмотренных законом о персональных данных

6.4.1. Учреждение принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных законом о персональных данных. Учреждение самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством, если иное не предусмотрено законом о персональных данных или другими федеральными законами. К таким мерам, в частности, относятся:

а) назначение лица, ответственного за организацию обработки персональных данных;

б) издание документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

в) применение необходимых правовых, организационных и технических мер по защите персональных данных от неправомерного или случайного доступа к ним,

уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении них; обеспечение безопасности персональных данных достигается, в частности:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) применением для уничтожения персональных данных прошедших в установленном порядке процедуру оценки соответствия средств защиты информации, в составе которых реализована функция уничтожения информации;

5) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных;

б) учетом машинных носителей персональных данных;

7) соблюдением условий хранения носителей персональных данных, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;

8) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

9) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

10) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

11) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

12) определением мест хранения материальных носителей персональных данных (в случае обработки персональных данных без использования средств автоматизации);

13) обеспечением отдельного хранения материальных носителей персональных данных, обработка которых осуществляется в различных целях (в случае обработки персональных данных без использования средств автоматизации).

г) осуществление внутреннего контроля и (или) аудита соответствия обработки законодательству, Положению и иным локальным нормативным актам Учреждения;

д) оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения закона о персональных данных, соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение выполнения обязанностей, предусмотренных законом о персональных данных;

е) ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства в области персональных данных, в том числе требованиями к защите персональных данных, Положением, иными локальными нормативными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.