

УТВЕРЖДАЮ

Главный врач
ГБУЗ "ГП №1 Г.
НОВОРОССИЙСКА" МЗ КК

 А.П. Гречишников
« 23 » _____ 2020 года

ПОЛОЖЕНИЕ

о порядке обработки персональных данных субъектов персональных данных ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ "ГОРОДСКАЯ ПОЛИКЛИНИКА №1 ГОРОДА НОВОРОССИЙСКА" МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ КРАСНОДАРСКОГО КРАЯ

1. Основные понятия

Для целей настоящего Положения используются следующие основные понятия:

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

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

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

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

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

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

обработка персональных данных – любое действие (операция) или

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

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

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

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

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

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

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

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

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

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

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

2. Общие положения

2.1. Цель разработки настоящего Положения – обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2.2. Положение разработано в соответствии со следующими нормативно-правовыми документами Российской Федерации:

1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» в рамках, определяемых данным Федеральным законом, заявлений;

2) Конституция Российской Федерации;

3) Гражданский кодекс Российской Федерации;

4) Кодекс об Административных Правонарушениях Российской Федерации;

5) Трудовой кодекс Российской Федерации;

6) Уголовный кодекс Российской Федерации;

7) Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

8) Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

9) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188;

10) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;

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

2.3. Под обработкой персональных данных понимается 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.

2.4. Положение определяет необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Состав целей обработки, категорий персональных данных, и способов обработки персональных данных определены в «Политике обработки персональных данных». Также «Политика обработки персональных данных» устанавливает перечень третьих лиц, которым передаются персональные данные или поручается их обработка.

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

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.

2.5. Деятельность по организации обработки и защиты персональных данных в соответствии с требованиями законодательства Российской Федерации о персональных данных осуществляет работник ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ ЗДРАВООХРАНЕНИЯ "ГОРОДСКАЯ ПОЛИКЛИНИКА №1 ГОРОДА НОВОРОССИЙСКА" МИНИСТЕРСТВА ЗДРАВООХРАНЕНИЯ КРАСНОДАРСКОГО КРАЯ (далее – Учреждение), ответственный за организацию обработки персональных данных Учреждения.

Деятельность по администрированию средств и механизмов защиты осуществляет работник, назначенный администратором информационной безопасности приказом главного врача.

Техническое обслуживание информационных систем персональных данных осуществляет работник, назначенный ответственным за техническое обслуживание информационных систем персональных данных приказом главного врача.

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

2.6. Учреждение может поручить обработку персональных данных третьим лицам с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом

соответствующего акта (далее – поручение Учреждения). Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении Учреждения, должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению Учреждения, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случаях, когда Учреждение поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

Учреждение и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.7. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Учреждение вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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

2.9. Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законодательством.

2.10. Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.

2.11. Все изменения в Положение вносятся приказом главного врача.

3. Порядок обработки персональных данных

3.1. Все персональные данные субъектов Учреждение получает от них самих либо от их законных представителей.

3.2. Обработка персональных данных осуществляется на законной и справедливой основе, а также с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ на основании согласия субъекта персональных данных на обработку его персональных данных, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Форма согласия утверждается приказом главного врача. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

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

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

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. 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.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

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

3.4. Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия. Форма согласия утверждается приказом главного врача. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

Персональные данные могут быть получены Учреждением от лица, не являющегося субъектом персональных данных, при условии предоставления Учреждения подтверждения наличия оснований, указанных в Федеральном законе № 152-ФЗ.

3.5. Персональные данные субъектов Учреждения обрабатываются в структурных подразделениях в соответствии с исполняемыми ими функциями

и обязанностями.

3.6. Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком допущенных лиц, утверждённом в порядке, определяемом в Учреждении.

3.7. Доступ к персональным данным, обрабатываемым в информационных системах персональных данных (далее - ИСПДн), осуществляется в соответствии со списком допущенных лиц, утверждённом в порядке, определяемом в Учреждении.

3.8. Уполномоченные лица, допущенные к персональным данным субъектов Учреждения, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностной инструкцией уполномоченных лиц.

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

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

3.10. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

3.11. Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются приказом об утверждении мест хранения материальных носителей персональных данных Учреждения.

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

1) выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных;

2) 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;

3) выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения и невозможности обеспечить правомерную обработку персональных данных;

4) достижения целей обработки или в случае утраты необходимости в их достижении;

5) отзыва согласия субъекта персональных данных на обработку его персональных данных;

б) представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными, неактуальными (устаревшими), незаконно полученными или не являются необходимыми для заявленной цели обработки.

3.13. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного 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.

3.14. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его законного 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.

В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных субъектом персональных данных или его законным 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 7 рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

3.15. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением или лицом, действующим по поручению Учреждения, Учреждение в срок, не превышающий 3-х рабочих дней с даты этого выявления, осуществляет прекращение неправомерной обработки 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 10 рабочих дней с даты выявления неправомерной обработки персональных данных, осуществляет уничтожение таких персональных данных или обеспечивает их

уничтожение. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение субъекта персональных данных или его законного представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.16. 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 30 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 оператором и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

3.17. 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 30 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 Федеральным законом № 152-ФЗ или другими федеральными законами.

3.18. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения.

В срок, не превышающий 7 рабочих дней со дня представления

субъектом персональных данных или его законным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Учреждение уничтожает такие персональные данные. При этом Учреждение уведомляет субъекта персональных данных или его законного представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

3.19. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанные в пунктах 3.15 – 3.18, Учреждение осуществляет блокирование таких персональных данных 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 6 месяцев, если иной срок не установлен федеральными законами.

3.20. Уничтожение персональных данных осуществляет комиссия в составе руководителя и работников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

3.21. Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

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

При этом составляется акт, подписываемый председателем комиссии, проводившей уничтожение материальных носителей персональных данных.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Учреждения должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

3.22. Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

3.23. Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, работники структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

3.24. Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях) или путем механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется «Акт уничтожения полей баз данных Учреждения, содержащих персональные данные субъекта». Форма акта утверждается отдельным приказом.

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

3.26. При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных, допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была не возможна.

3.27. Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

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

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

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ.

Форма согласия утверждается приказом главного врача. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

3.29. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

3.30. Работник должны быть ознакомлены под подпись с настоящим

Положением и другими документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

4. Правила работы с обезличенными данными

4.1. Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации, установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утверждены Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Методические рекомендации содержат анализ процессов автоматизированной обработки обезличенных данных, требования к обезличенным данным и методам обезличивания, позволяющей выделить основные свойства обезличенных данных и методов обезличивания и оценить возможность их применения при решении задач обработки персональных данных с учетом вида деятельности Оператора и необходимых действий с персональными данными.

4.2. К наиболее перспективным и удобным для практического применения относятся один из следующих методов обезличивания:

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

2). метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

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

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

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

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

4.4. В случае, если обезличенные персональные данные используются в

статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Учреждения исходя из служебной необходимости, и получение согласия субъекта на обработку его персональных данных не требуется на основании пункта 9 части 1 статьи 6 Федерального закона № 152-ФЗ.

4.5. Если обезличенные персональные данные используются в целях продвижения товаров, работ, услуг на рынке, или в целях политической агитации, Учреждение обязана получить согласие субъекта персональных данных на подобную обработку.

5. Передача персональных данных третьим лицам

5.1. При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта;

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

5.2. При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Учреждение запрашивает согласие субъекта в письменной форме. Форма согласия утверждается приказом главного врача. Допускается совмещение формы согласия субъекта с типовой формой документов, содержащих персональные данные субъекта (например: анкеты). Допускается совмещение формы согласия субъекта с другими формами согласий.

6. Права субъектов персональных данных

6.1. В целях обеспечения своих законных интересов субъекты персональных данных или его представители имеют право:

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

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ;

3) требовать уточнение его персональных данных, их блокирование или уничтожение в случаях, 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. Субъект персональных

данных при отказе Учреждения исключить или исправить, заблокировать или уничтожить его персональные данные имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;

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

5) обжаловать в суде или в уполномоченном органе по защите прав субъектов персональных данных любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта персональных данных, если субъект персональных данных считает, что Учреждение осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы.

6.2. В случае, если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Учреждения или направить ему повторный запрос в целях получения сведений, и ознакомления с персональными данными не ранее, чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

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

6.3. Учреждение вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Учреждении.

6.4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской Федерации.

7. Порядок обработки обращений и запросов субъектов

7.1. При обращении либо письменном запросе субъекта персональных данных или его законного представителя, на доступ к своим персональным данным Учреждение руководствуется требованиями статей 14, 18 и 20 Федерального закона № 152-ФЗ;

7.2. Доступ субъекта персональных данных или его законного представителя к своим персональным данным Учреждение предоставляет только под контролем ответственного за организацию обработки персональных данных Учреждения.

7.3. Обращение субъекта персональных данных или его законного представителя фиксируются в журнале учета обращений граждан (субъектов персональных данных) по вопросам обработки персональных данных.

7.4. Письменный запрос субъекта персональных данных или его законного представителя фиксируются в журнале регистрации письменных запросов граждан на доступ к своим персональным данным.

7.5. Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекту персональных данных или его законному представителю к персональным данным указанного субъекта.

7.6. В случае, если данные предоставленные субъектом персональных данных или его законным представителем недостаточны для установления его личности или предоставление персональных данных нарушают конституционные права и свободы других лиц ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

7.7. Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает работника (работников) структурного подразделения, обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения.

Учреждение предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение осуществляет в них необходимые изменения. В срок, не превышающий 7 рабочих дней со дня предоставления 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.

7.8. Сведения о наличии персональных данных Учреждение предоставляет субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

7.9. Сведения о наличии персональных данных должны быть предоставлены субъекту при ответе на запрос в течение 30 дней от даты получения запроса субъекта персональных данных или его законного представителя.

8. Порядок действий в случае запросов надзорных органов

8.1. В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

8.2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников Учреждения.

8.3. В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

9. Защита персональных данных субъекта

9.1. Защиту персональных данных субъектов от неправомерного их использования или утраты Учреждение обеспечивает за счет собственных средств в порядке, установленном законодательством Российской Федерации.

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

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

1) руководящим документом ФСТЭК России - «Состав и содержание организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных». Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

3) внутренними документами Учреждения, действующими в сфере обеспечения информационной безопасности.

9.2. Защита персональных данных предусматривает ограничение к ним доступа.

9.3. Руководитель структурного подразделения Учреждения, осуществляющего обработку персональных данных:

1) несет ответственность за организацию защиты персональных данных в подчиненном структурном подразделении;

2) закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций и задач;

3) организует изучение подчиненными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

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

5) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями работников подразделения.

9.4. Работники допущенные к персональным данным дают письменное обязательство о неразглашении таких данных в установленном порядке.

10. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Учреждения по обработке и защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закрепленных за ними носителей персональных данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю отдела (структурного подразделения) обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

Ответственный за организацию обработки персональных данных Учреждения организует проведение инструктажа и ознакомление работников Учреждения, 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.

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

11.1. Лица, виновные в нарушении норм, регулирующих получение, обработку, передачу и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности.

11.2. К данным лицам могут быть применены следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) предупреждение о неполном должностном соответствии;
- 4) освобождение от занимаемой должности;
- 5) увольнение.

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

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

11.5. Если в течение года со дня применения дисциплинарного взыскания работник не будет подвергнут новому дисциплинарному взысканию, то он считается не имеющим дисциплинарного взыскания. Учреждение до истечения года со дня издания приказа о применении дисциплинарного взыскания, имеет право снять его с работника по собственной инициативе, по письменному заявлению работника или по ходатайству его непосредственного руководителя.

Главный врач



А.П. Гречишников