Защита персональных данных

Полный комплект локальных документов медорганизации, которые защитят от штрафов

«АКТИОН» МЦФЭР

ПРАВОВЫЕ ВОПРОСЫ
В ЗДРАВООХРАНЕНИИ

Содержание

12

форм документов,
которые понадобятся медорганизации, чтобы пройти проверку Роскомнадзора по работе с персональными данными

Автор-составитель

Елена ХМЕЛЕВСКАЯ, адвокат, советник специализированной юридической компании «Росмедконсалтинг», Санкт-Петербург

Политика обработки персональных данных. Образец

УТВЕРЖДЕНА
приказом
от «___»_____ 20__ г. № ____

Политика
обработки персональных данных

1. Общие положения

1.1. Настоящая политика в отношении обработки персональных данных (далее – Политика) разработана _____
(наименование медицинской организации)
(далее – Оператор) в целях исполнения требований Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных».

Политика определяет общий порядок, принципы и условия обработки персональных данных Оператором и обеспечивает защиту прав субъектов персональных данных при обработке их персональных данных.

1.2. Основные понятия, используемые в Политике:
- *персональные данные.* Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- *оператор персональных данных (оператор).* Учреждение, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- *обработка персональных данных*. Любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их исполь-

Медорганизация должна разместить Политику обработки персональных данных в уголке потребителя и на сайте.

зования. Обработка персональных данных включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

- *автоматизированная обработка персональных данных*. Обработка персональных данных с помощью средств вычислительной техники;
- *распространение персональных данных*. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- *предоставление персональных данных*. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- *блокирование персональных данных*. Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- *уничтожение персональных данных*. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- *обезличивание персональных данных*. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- *информационная система персональных данных*. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- *трансграничная передача персональных данных*. Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- *субъект персональных данных*. Физическое лицо, данные которого обрабатываются;
- *конфиденциальность персональных данных*. Обязательное для оператора и иных лиц, получивших 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.

2. Основные права и обязанности Оператора персональных данных

2.1. Оператор при сборе персональных данных обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных.

2.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

2.3. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети интернет, Оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных Федеральном законе «О персональных данных».

2.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

2.5. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике, к сведениям о реализуемых требованиях к защите персональных данных. Оператор в случае осуществления сбора персональных данных с использованием информационно-телекоммуникационных сетей обязан опубликовать в соответствующей информационно-телекоммуникационной сети Политику и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием соответствующей информационно-телекоммуникационной сети.

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

2.7. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Оператора 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 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 «О персональных данных».

3. Основные права и обязанности субъекта персональных данных

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

3.2. 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 допускается только при условии предварительного согласия субъекта персональных данных.

3.3. 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 разрешается только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

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

3.5. 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.

4. Цели сбора персональных данных

4.1. Оператор обрабатывает персональные данные в целях:
- оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества;
- заключения, исполнения и прекращения гражданско-правовых договоров;
- оказания медицинских услуг, в том числе идентификации пациентов (заказчиков), отражения информации в медицинской документации, предоставления сведений страховым компаниям (в случае

оплаты ими оказываемых услуг), предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг;
- выполнения требований действующего законодательства;
- в иных случаях, установленных в законе, уставе Оператора.

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

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

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

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

4.6. 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.

5. Правовые основания обработки персональных данных

5.1. Правовым основанием обработки персональных данных является совокупность правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных.

5.2. Оператор обрабатывает персональные данные на основании:
- Трудового кодекса Российской Федерации;
- Федерального закона «Об основах охраны здоровья граждан в Российской Федерации» и принятых на его основе нормативно-правовых

актов, регулирующих отношения, связанные с оказанием медицинских услуг;
- иных федеральных законов и прочих нормативных правовых актов;
- устава Оператора;
- договоров, заключаемых между Оператором и субъектами персональных данных;
- согласий на обработку персональных данных.

6. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

6.1. Категории субъектов персональных данных, чьи данные обрабатываются.

6.1.1. Работники Оператора, бывшие работники, кандидаты на трудоустройство, а также члены семьи работников.

6.1.2. Пациенты, законные представители пациентов.

6.1.3. Прочие клиенты и контрагенты Оператора (физические лица).

6.1.4. Представители/работники клиентов и контрагентов Оператора (юридических лиц).

6.2. В отношении категории, указанной в пункте 6.1.1 (за исключением членов семьи работников), обрабатываются:
- фамилия, имя, отчество;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- гражданство;
- образование;
- профессия, должность;
- стаж работы;
- семейное положение, наличие детей;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

– данные страхового свидетельства государственного пенсионного страхования;
– идентификационный номер налогоплательщика;
– табельный номер;
– сведения о доходах;
– сведения о воинском учете;
– сведения о судимостях;
– сведения о повышении квалификации, о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях;
– сведения о социальных гарантиях;
– сведения о состоянии здоровья, влияющие на выполнение трудовой функции.

6.3. Персональные данные родственников работников обрабатываются в объеме, переданном работником и необходимом для предоставления гарантий и компенсаций работнику, предусмотренных трудовым законодательством:
– фамилия, имя, отчество;
– дата и место рождения;
– серия и номер документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
– серия и номер свидетельства о рождении ребенка, сведения о выдаче указанного документа и выдавшем его органе;
– серия и номер свидетельства о заключении брака, сведения о выдаче указанного документа и выдавшем его органе.

6.4. В отношении пациентов обрабатываются:
– фамилия, имя, отчество;
– пол;
– возраст;
– дата и место рождения;
– адреса места жительства и регистрации;
– серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;

– данные страхового свидетельства государственного пенсионного страхования;
– гражданство;
– данные о состоянии здоровья, в том числе биометрические персональные данные;
– семейное и социальное положение;
– контактный телефон;
– адрес электронной почты;
– реквизиты полиса обязательного медицинского страхования;
– реквизиты полиса (договора) добровольного медицинского страхования;
– тип занятости;
– место работы;
– должность.

6.5. В отношении категорий, указанных в пунктах 6.1.3 и 6.1.4, обрабатываются:
– фамилия, имя, отчество;
– пол;
– возраст;
– дата и место рождения;
– адреса места жительства и регистрации;
– контактный телефон;
– адрес электронной почты;
– серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе.

6.6. В отношении законных представителей или представителей по доверенности указанных лиц обрабатываются:
– фамилия, имя, отчество;
– пол;
– возраст;
– дата и место рождения;
– адреса места жительства и регистрации;
– контрактный телефон;
– адрес электронной почты;

– серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
– сведения о документе, который подтверждает полномочия представителя.

7. Порядок и условия обработки персональных данных

7.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

7.2. Оператор не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона «О персональных данных».

7.3. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью.

7.4. Письменное согласие субъекта персональных данных должно включать:
– фамилию, имя, отчество;
– адрес субъекта персональных данных;
– номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
– наименование и адрес Оператора;
– цель обработки персональных данных;
– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;
– срок, в течение которого действует согласие;
– способ его отзыва;
– подпись субъекта персональных данных.

7.5. Обработка персональных данных осуществляется Оператором следующими способами:
- неавтоматизированная обработка персональных данных;
- автоматизированная обработка персональных данных с передачей полученной информации по информационно-телекоммуникационным сетям или без таковой;
- смешанная обработка персональных данных.

7.6. Оператор организует обработку персональных данных в следующем порядке:

1) назначает ответственного за организацию обработки персональных данных, устанавливает перечень лиц, имеющих доступ к персональным данным;

2) издает настоящую Политику, локальные акты по вопросам обработки персональных данных;

3) применяет правовые, организационные и технические мер по обеспечению безопасности персональных данных;

4) осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящей Политике, локальным актам Оператора;

5) осуществляет оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», определяет соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных данным Федеральным законом;

6) знакомит работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите

персональных данных, настоящей Политики, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

7.7. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры, в том числе:

1) определяет угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

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

3) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации;

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

5) учитывает машинные носители персональных данных;

6) обнаруживает факты несанкционированного доступа к персональным данным и принимает меры;

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

8) устанавливает правила доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с пер-

сональными данными в информационной системе персональных данных.

7.8. При обработке персональных данных Оператор выполняет, в частности, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

7.9. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками Оператора, осуществляющими данную работу в соответствии с трудовыми обязанностями.

7.10. Оператор получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Оператором, а также в случаях, установленных федеральным законом.

7.11. Запрещается хранение документов с персональными данными и их копий на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

7.12. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

7.13. При увольнении работника, имеющего доступ к персональным данным, прекращении доступа к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

8. Порядок обработки персональных данных в информационных системах

8.1. Обработка персональных данных в информационных системах осуществляется после реализации организационных и технических мер по обеспечению безопасности персональных данных, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

8.2. Обеспечение безопасности при обработке персональных данных, содержащихся в информационных системах органов и подведомственных организаций, осуществляется в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

8.3. Уполномоченному работнику, имеющему право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе. Доступ предоставляется в соответствии с функциями, предусмотренными должностными обязанностями работника.

8.4. Информация может вноситься как в автоматическом режиме при получении персональных данных с официального сайта в сети интернет, так и в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

8.5. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах органов, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

8.6. В случае выявления нарушений порядка обработки персональных данных уполномоченными работниками незамедлительно принимаются меры по установлению причин нарушений и их устранению.

8.7. В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации и технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

8.8. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных».

8.9. В соответствии с пунктом 11 статьи 19 Федерального закона «О персональных данных» под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

При обработке персональных данных в информационных системах устанавливаются четыре уровня защищенности персональных данных.

8.9.1. Необходимость обеспечения первого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает либо специальные категории персональ-

ных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

8.9.2. Необходимость обеспечения второго уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы первого типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

в) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

д) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

е) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

8.9.3. Необходимость обеспечения третьего уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает общедоступные персональные данные сотрудников Оператора или общедоступные персональные данные менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

б) для информационной системы актуальны угрозы второго типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

в) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает специальные категории персональных данных сотрудников Оператора или специальные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора;

г) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных более чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

8.9.4. Необходимость обеспечения четвертого уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы третьего типа и информационная система обрабатывает иные категории персональных данных сотрудников Оператора или иные категории персональных данных менее чем 100 000 субъектов персональных данных, не являющихся сотрудниками Оператора.

8.10. Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21.

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

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

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения Оператора, сведения о лицах (за исключением работников Оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

10) иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

9.2. Указанные выше сведения должны быть предоставлены субъекту персональных данных Оператором в доступной форме и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

9.3. Сведения, указанные в пункте 9.1, предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе,

сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

9.4. В случае если сведения, указанные в пункте 9.1, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 9.1, и ознакомления с такими 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.

9.5. Субъект персональных данных вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений, указанных в пункте 9.1, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 9.4, 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 со сведениями, указанными в пункте 9.1, должен содержать обоснование направления повторного запроса.

9.6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 9.4 и 9.5. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе.

9.7. Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 дней с даты получения запроса субъекта персональных данных или его представителя.

9.8. Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

9.9. 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, Оператор обязан внести в них необходимые изменения.

9.10. 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, Оператор обязан уничтожить такие персональные данные.

9.11. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

9.12. 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 Оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персо-

нальных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) с момента такого обращения или получения указанного запроса на период проверки.

9.13. 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 Оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) 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.

9.14. В случае подтверждения факта неточности персональных данных Оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

9.15. В случае выявления неправомерной обработки персональных данных, осуществляемой Оператором или лицом, действующим по поручению Оператора, Оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Оператор в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уни-

чтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить 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.

9.16. В случае достижения цели обработки персональных данных Оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) 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 Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

9.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) 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 Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

9.18. В случае отсутствия возможности уничтожения персональных данных в течение указанных сроков Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

10. Заключительные положения

10.1. Политика является общедоступным документом.

10.2. Ответственность лиц, имеющих доступ к персональным данным, определяется действующим законодательством Российской Федерации.

Положение об обработке персональных данных работников. Образец

УТВЕРЖДЕНО
приказом
от «___»_____ 20__ г. № ____

Положение
об обработке персональных данных работников

1. Общие положения

1.1. Настоящее Положение об обработке персональных данных работников (далее – Положение) разработано _____
(наименование медицинской организации)

(далее – Работодатель) в целях определения порядка обработки персональных данных работников; обеспечения защиты прав и свобод работников при обработке их персональных данных, а также установления ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Перечень основных определений:
- *персональные данные*. Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- *обработка персональных данных*. Любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования.

Клиника обрабатывает персональные данные не только пациентов, но и работников. Правила следует прописать в Положении об обработке персональных данных работников.

Обработка персональных данных включает в себя сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

- *автоматизированная обработка персональных данных*. Обработка персональных данных с помощью средств вычислительной техники;
- *распространение персональных данных*. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- *предоставление персональных данных*. Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- *блокирование персональных данных*. Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
- *уничтожение персональных данных*. Действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- *обезличивание персональных данных*. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- *информационная система персональных данных*. Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- *трансграничная передача персональных данных*. Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;
- *субъект персональных данных*. Физическое лицо, данные которого обрабатываются;
- *конфиденциальность персональных данных*. Обязательное для Работодателя и иных лиц, получивших 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.

1.4. Сведения о персональных данных работников относятся к числу конфиденциальных и составляют охраняемую законом тайну.

2. Состав персональных данных

2.1. Работодатель может обрабатывать следующие персональные данные работника:
- фамилия, имя, отчество;
- дата и место рождения;
- адреса места жительства и регистрации;
- контактный телефон;
- гражданство;
- образование;
- профессия, должность, стаж работы;
- семейное положение, наличие детей;
- серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе;
- данные страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- табельный номер;
- сведения о доходах;
- сведения о воинском учете;
- сведения о судимостях;
- сведения о повышении квалификации, о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о социальных гарантиях;
- сведения о состоянии здоровья, влияющие на выполнение трудовой функции.

2.2. У Работодателя создаются и хранятся следующие документы, содержащие персональные данные работников:

– документы, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
– личные дела и трудовые книжки работников;
– подлинники и копии приказов (распоряжений) по личному составу;
– документы, связанные с выплатой заработной платы;
– справочно-информационные данные по персоналу, картотеки, журналы;
– подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству учреждения;
– копии отчетов, направляемых в предусмотренных законом случаях в государственные органы статистики, налоговые инспекции и другие органы (организации).

3. Условия обработки персональных данных

3.1. Обработка персональных данных осуществляется после принятия необходимых мер по защите персональных данных.

3.2. Работодатель не вправе обрабатывать персональные данные субъекта персональных данных без его письменного согласия, за исключением случаев, предусмотренных статьей 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей).

3.3. Письменное согласие субъекта персональных данных должно включать:
– фамилию, имя, отчество;
– адрес субъекта персональных данных;
– номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
– наименование и адрес Работодателя;
– цель обработки персональных данных;
– перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Работодателем способов обработки персональных данных;
– срок, в течение которого действует согласие;
– способ отзыва согласия;
– подпись субъекта персональных данных.

3.4. Работодатель назначает работника, ответственного за организацию обработки персональных данных, устанавливает перечень лиц, допущенных к обработке персональных данных.

3.5. Лица, допущенные к обработке персональных данных, подписывают обязательство о неразглашении персональных данных.

4. Обработка персональных данных

4.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативно-правовых актов, оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества.

4.2. Обработка персональных данных в информационных системах персональных данных осуществляется в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных документов уполномоченных федеральных органов исполнительной власти.

4.3. Обработка персональных данных, осуществляемая без использования средств автоматизации, считается таковой, если такие действия с персональными данными осуществляются при непосредственном участии человека. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется в соответствии

с требованиями постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.4. Документы, содержащие персональные данные, должны обрабатываться в служебных помещениях с ограничением доступа.

4.5. Работодатель получает персональные данные непосредственно от субъектов персональных данных или их представителей, наделенных соответствующими полномочиями.

4.6. Субъект персональных данных обязан предоставлять достоверные сведения.

4.7. При изменении персональных данных работник письменно уведомляет Работодателя о таких изменениях в срок, не превышающий 14 дней с момента их изменения. Данное обязательство не распространяется на изменение персональных данных, предоставление которых требует соответствующего согласия работника.

4.8. Согласия субъекта на получение его персональных данных от третьих лиц не требуется в случаях, когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде, а также в случаях, установленных федеральным законом.

4.9. В целях обеспечения сохранности и конфиденциальности персональных данных все операции с персональными данными должны выполняться только работниками учреждения, осуществляющими данную работу в соответствии с трудовыми обязанностями.

4.10. Запрещается хранить документы, содержащие персональные данные, и их копии на рабочих местах и (или) в открытом доступе, оставлять шкафы (сейфы) открытыми в случае выхода работника из рабочего помещения.

4.11. В электронном виде документы, содержащие персональные данные, разрешается хранить в специализированных базах данных или в специ-

ально отведенных для этого директориях с ограничением и разграничением доступа. Копирование таких данных запрещено.

4.12. При увольнении работника, имеющего доступ к персональным данным, документы и иные носители, содержащие персональные данные, сдаются работником своему непосредственному руководителю.

4.13. Передача персональных данных между структурными подразделениями осуществляется только между работниками, имеющими доступ к персональным данным.

4.14. Персональные данные в соответствии с нормами действующего законодательства могут передаваться в государственные и негосударственные органы и учреждения, в частности:
- налоговые органы;
- органы социального страхования;
- органы государственной власти в сфере занятости населения;
- военкоматы;
- банк, в который перечисляется заработная плата в соответствии с заявлением работника;
- правоохранительные и судебные органы;
- профсоюзные органы.

Передача персональных данных третьим лицам осуществляется только с письменного согласия субъекта, за исключением случаев, установленных федеральными законами.

Персональные данные передаются с обязательным уведомлением лица, получающего их, об обязанности использования полученной конфиденциальной информации лишь в целях, для которых она сообщена, и с предупреждением об ответственности за незаконное использование данной информации в соответствии с федеральными законами.

4.15. Персональные данные подлежат уничтожению по достижении целей обработки, в случае утраты необходимости в их достижении или по истечении установленных сроков их хранения.

5. Ответственность

5.1. С правилами работы и хранения персональных данных в обязательном порядке должны быть ознакомлены все работники учреждения.

5.2. Работник, которому в силу трудовых отношений стала известна информация, составляющая персональные данные, в случае нарушения режима защиты этих данных несет материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Приказ об утверждении Политики обработки персональных данных. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

Об утверждении Политики обработки персональных данных

С целью организации обработки персональных данных работников в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Политику обработки персональных данных (прилагается).

2. Документ ввести в действие с «___»_____ 20__г.

3. Разместить документ на сайте организации в сети интернет и на информационном стенде.

Ответственный: _____
(должность, Ф. И. О.)

4. Ознакомить работников с документом под подпись.

Ответственный: _____
(должность, Ф. И. О.)

Утвердите приказом Политику обработки персональных данных и ознакомьте сотрудников с документом под подпись.

5. Контроль за исполнением приказа возложить на _____

_____

(должность, Ф. И. О.)

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

С приказом ознакомлен(ы):

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

Приказ об утверждении Положения об обработке персональных данных работников. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

Об утверждении Положения
об обработке персональных данных работников

С целью организации обработки персональных данных работников в соответствии с требованиями Трудового кодекса Российской Федерации и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке персональных данных работников (прилагается).

2. Документ ввести в действие с «__»_____20__ г.

3. Ознакомить работников с документом под подпись.

Ответственный: _____
(должность, Ф. И. О.)

4. Контроль за исполнением приказа возложить на _____
_____
(должность, Ф. И. О.)

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

Утвердите приказом Положение об обработке персональных данных работников и ознакомьте сотрудников с документом под подпись.

С приказом ознакомлен(ы):

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

Согласие на обработку персональных данных работника. Образец

Согласие на обработку персональных данных

Я, _____,
(Ф. И. О. полностью)

зарегистрированный по адресу: _____.

Документ, удостоверяющий личность: _____
_____.
(серия и номер документа, кем и когда выдан)

Настоящим выражаю согласие на обработку моих персональных данных _____ (далее – Оператор), находящемуся по адресу:
(наименование учреждения)

_____,
для целей обеспечения соблюдения законов и иных нормативных правовых актов, оформления трудовых отношений, ведения кадрового делопроизводства, содействия в трудоустройстве, обучении, повышении по службе, пользовании различными льготами и гарантиями, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и сохранности имущества.

Для указанных целей могут быть получены сведения: фамилия, имя, отчество, дата и место рождения, адреса места жительства и регистрации, контактный телефон, гражданство, образование, профессия, должность, стаж работы, семейное положение, наличие детей, серия и номер основного документа, удостоверяющего личность, сведения о выдаче указанного документа и выдавшем его органе, данные страхового свидетельства государственного пенсионного страхования, идентификационный номер налогоплательщика, табельный номер, сведения о доходах, сведения о воинском учете, сведения о судимостях, сведения о повышении квалификации, о профессиональной переподготовке, сведения о наградах (по-

Обрабатывать персональные данные можно с письменного согласия работника. Форму согласия скорректируйте с учетом специфики вашей медорганизации, уточните категории обрабатываемых данных.

ощрениях), почетных званиях, сведения о социальных гарантиях, сведения о состоянии здоровья, влияющие на выполнение трудовой функции.

Я выражаю согласие:

- на получение моих персональных данных о предыдущих местах работы и периодах трудовой деятельности от третьих лиц с целью сбора информации о моем опыте работы;
- включение в общедоступные источники следующих персональных данных работников (на информационным стенде и сайте Оператора): Ф. И. О., сведения о профессии, должности, квалификации.

В отношении персональных данных я даю Оператору согласие на совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, иных действий, предусмотренных действующим законодательством, совершаемых как с использованием средств автоматизации, так и без использования таковых, в том объеме, который необходим для достижения целей обработки, указанных в настоящем согласии.

Настоящее согласие вступает в силу с момента его подписания и действует в течение всего срока рассмотрения моей кандидатуры при трудоустройстве, а в случае заключения трудового договора – в течение срока действия моего трудового договора либо установленного в законодательстве срока хранения документов, содержащих мои персональные данные. Настоящее согласие может быть отозвано путем подачи Оператору письменного заявления.

_____ _____

(подпись) (Ф. И. О. полностью)

«____» _____ 20__ г.

Согласие на обработку персональных данных пациента. Образец

Согласие на обработку персональных данных

Я, _____,
(Ф. И. О. субъекта персональных данных)

зарегистрированный по адресу: _____.

Документ, удостоверяющий личность _____.
(серия и номер документа, кем и когда выдан)

В соответствии со статьями 9, 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» даю согласие на обработку моих персональных данных _____
(наименование учреждения)

(далее – Оператор), находящемуся по адресу: _____, в целях оказания мне медицинских услуг и иных услуг, в том числе идентификации, отражения информации в медицинской документации, предоставления сведений страховым компаниям (в случае оплаты ими оказываемых услуг), предоставления установленной законодательством отчетности в отношении оказанных медицинских услуг.

Перечень персональных данных, на обработку которых я даю согласие: фамилия, имя, отчество, пол, возраст, дата и место рождения, адрес, паспортные данные, СНИЛС, гражданство, данные о состоянии здоровья, в том числе биометрические персональные данные, семейное, социальное положение,

Обрабатывать персональные данные можно с письменного согласия субъекта или в случаях, которые устанавливает часть 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Если обрабатываете данные только для того, чтобы оказать медпомощь, можно обойтись без письменного согласия. Однако медорганизация обычно работает с объемом, который превышает перечень закона. Например, использует данные для отправки пациенту СМС с напоминанием о предстоящем визите, для создания сервиса «Личный кабинет» на сайте медорганизации и т. д. Поэтому письменное согласие лучше брать всегда. Скорректируйте форму согласия с учетом особенностей вашей медорганизации.

контактный телефон, адрес электронной почты, реквизиты полиса ОМС (ДМС), образование, тип занятости, место работы, должность, другая информация, содержащаяся в относящихся ко мне документах и иных источниках, предоставленных Оператору или полученных им в установленном законом порядке.

В отношении указанных персональных данных я даю Оператору согласие на совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), в том числе трансграничную, обезличивание, блокирование, удаление, уничтожение персональных данных, иных действий, предусмотренных действующим законодательством, совершаемых как с использованием средств автоматизации, так и без использования таковых, в том объеме, который необходим для достижения целей обработки, указанных в настоящем согласии.

Настоящее согласие действует со дня подписания до дня его отзыва либо на срок хранения документации, установленный в законодательстве. Настоящее согласие может быть отозвано путем подачи Оператору письменного заявления.

Раздел заполняется, если согласие подписывает законный представитель недееспособного лица или представитель по доверенности

_____,
(Ф. И. О. представителя субъекта персональных данных)

зарегистрированный по адресу: _____.

Документ, удостоверяющий личность _____
_____
(серия и номер документа, кем и когда выдан)

Документ, подтверждающий полномочия представителя: _____
_____
(серия и номер документа, кем и когда выдан)

_____ _____
(подпись) (Ф. И. О. полностью)

«____» _____ 20__ г.

Приказ о назначении ответственного за организацию обработки персональных данных. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

**О назначении ответственного
за организацию обработки персональных данных**

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных _____.
(должность, Ф. И. О.)

2. Контроль за исполнением приказа оставляю за собой.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

С приказом ознакомлен:

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

Руководитель медорганизации должен назначить ответственного за организацию обработки персональных данных (п. 1 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

Приказ об утверждении перечня лиц, имеющих доступ к персональным данным. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

**Об утверждении перечня лиц,
имеющих доступ к персональным данным**

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Утвердить перечень лиц, имеющих доступ к персональным данным, обрабатываемым в организации (прилагается).

2. Определить объем их полномочий при работе с персональными данными.

3. Довести информацию до всех работников, допущенных к обработке персональных данных, под подпись.

4. Контроль за исполнением настоящего приказа оставляю за собой.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

Определите перечень сотрудников, которые имеют доступ к персональным данным, и объем их полномочий (п. 6 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

С приказом ознакомлен(ы):

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

«___»_____20__ г.

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

«___»_____20__ г.

_____ _____ _____
(должность) (подпись) (Ф. И. О.)

«___»_____20__ г.

Приложение

Перечень лиц, допущенных к обработке персональных данных

Должность	Фамилия, имя, отчество	Объем полномочий (полный/частичный доступ для выполнения трудовых обязанностей)
1.		
2.		
3.		
4.		
5.		

Обязательство о неразглашении персональных данных. Образец

Обязательство о неразглашении персональных данных

Я,_____,
(Ф. И. О. полностью)

настоящим подтверждаю, что я понимаю, что во время исполнения своих трудовых обязанностей я занимаюсь обработкой персональных данных, а также что разглашение такого рода информации может нанести ущерб субъектам обрабатываемых мною персональных данных и моему работодателю.

В связи с этим принимаю на себя обязательство при работе с персональными данными соблюдать все установленные в _____

_____
(наименование организации)

(далее – организация) требования по защите персональных данных, в том числе:

1. Не разглашать сведения, составляющие персональные данные, которые мне будут доверены или станут известны во время исполнения мною трудовых обязанностей.

2. Не использовать сведения, составляющие персональные данные, в личных целях и в целях извлечения выгоды.

3. Не передавать третьим лицам и не раскрывать публично сведения, составляющие персональные данные, без письменного разрешения субъектов персональных данных.

4. Выполнять относящиеся ко мне требования Политики обработки персональных данных, Положения об обработке персональных данных работников и иных локальных нормативных актов и приказов работодателя, касающихся вопросов обработки персональных данных.

Сотрудники, ответственные за организацию обработки персональных данных, и медработники, которые имеют доступ к этим данным, должны подписать обязательство о неразглашении персональных данных.

5. В случае попытки посторонних лиц получить от меня сведения о персональных данных немедленно сообщить об этом руководству организации.

6. В случае моего увольнения либо прекращения доступа к персональным данным в связи с переводом на другую должность или по иным причинам, все носители персональных данных, находившиеся в моем распоряжении, передать лицу, ответственному за организацию обработки персональных данных в организации.

7. Об утрате или недостаче носителей персональных данных, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), печатей и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможного разглашения персональных данных немедленно сообщать руководству организации.

Подписанием настоящего обязательства подтверждаю, что до моего сведения доведены положения действующего законодательства Российской Федерации, а также Политики обработки персональных данных, Положения об обработке персональных данных работников и иных локальных нормативных актов, касающихся вопросов обработки персональных данных.

Я предупрежден(а) о том, что в случае разглашения мною сведений, составляющих персональные данные, допущения при обработке персональных данных иных нарушений законодательства в области обработки персональных данных я несу дисциплинарную и материальную ответственность в порядке, установленном Трудовым кодексом Российской Федерации, а также гражданско-правовую, административную и уголовную ответственность в порядке, установленном федеральными законами.

_____ _____

(подпись) (Ф. И. О. полностью)

«____» _____ 20__ г.

Приказ об определении уровней защищенности информационных систем, содержащих персональные данные. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

Об определении уровней защищенности информационных систем, содержащих персональные данные

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Сформировать комиссию для оценки уровней защищенности информационных систем.

2. Председателем комиссии назначить _____
(должность, Ф. И. О.)

3. В состав комиссии включить следующих сотрудников:

_____
(должность, Ф. И. О.)

При обработке персональных данных в электронном виде медучреждение должно принимать технические меры по их защите. Оцените уровень безопасности медицинских информационных систем в зависимости от объема обрабатываемых данных, категорий и типов угроз. Для этого создайте комиссию.

_____
(должность, Ф. И. О.)

_____
(должность, Ф. И. О.)

4. Комиссии провести оценку организации защиты персональных данных, обрабатываемых учреждением. Учитывать категории и объем обрабатываемых персональных данных, категории субъектов персональных данных, категории информационных систем персональных данных, тип актуальных угроз.

5. Контроль за исполнением приказа оставляю за собой.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

С приказом ознакомлен(ы):

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

Приказ о внесении изменений в персональные данные. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

О внесении изменений в персональные данные

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с поступлением заявления о внесении изменений в персональные данные _____
(должность (при необходимости), Ф. И. О.)

ПРИКАЗЫВАЮ:

1. _____ внести изменения в персональные данные
(должность, Ф. И. О.)

_____на основании заявления (регистрационный
(должность, Ф. И. О.)

номер _____ от « ___» _____ 20__ г.). Срок: семь рабочих дней.

2. Письменно уведомить субъекта персональных данных о внесенных изменениях.

3. Контроль за исполнением приказа оставляю за собой.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

С приказом ознакомлен:

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

Если при обработке персональных данных потребовалось внести в них изменения, оформите это приказом.

Приказ об уничтожении персональных данных. Образец

_____
(наименование учреждения)

Приказ

«___»_____20__ г. № __

_____
(место издания)

Об уничтожении персональных данных

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и в связи с поступлением заявления о персональных данных, которые не являются необходимыми для заявленных целей обработки,

ПРИКАЗЫВАЮ:

1. _____ на основании заявления
(должность, Ф. И. О.)

от _____ (регистрационный номер
(должность (при необходимости), Ф. И. О.)

_____ от « ____» _____ 20__ г.) удалить из информационных систем персональные данные, которые не соответствуют целям обработки. Уничтожить печатные документы с аналогичными данными, если они не подлежат хранению.

2. Оформить акт уничтожения и представить его на утверждение руководителю организации. Срок: семь рабочих дней.

3. Письменно уведомить субъект персональных данных о факте уничтожения.

При работе с персональными данными может возникнуть необходимость их уничтожить. Издайте соответствующий приказ.

3. Контроль за исполнением приказа оставляю за собой.

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

С приказом ознакомлен:

_____	_____	_____
(должность)	(подпись)	(Ф. И. О.)

«___»_____20__ г.

Как Роскомнадзор проводит проверки и какие санкции возможны

Виды проверок

Проверки Роскомнадзора бывают плановые и внеплановые. График плановых проверок ведомство составляет на календарный год и публикует на rkn.gov.ru. Внеплановые проверки проводит, когда получает жалобы на медорганизацию.

Ревизии бывают документарные и выездные. В первом случае инспекторы просят выслать документы. Во втором – выезжают в медорганизацию.

Роскомнадзор запрашивает документы, которые содержат персональные данные. Например, договоры на оказание платных медуслуг. Также проверяет информационные системы и деятельность по обработке персональных данных. Единого списка документов, которые вправе смотреть инспекторы, нет. Многое зависит от того, какие персональные данные обрабатывает медорганизация и в каких информационных системах. Также имеет значение, сколько документов она утвердила. Многие вопросы можно урегулировать в одном документе или утвердить несколько по каждому вопросу.

О внеплановой выездной проверке Роскомнадзор обязан сообщить медорганизации за 24 часа. Если повод – информация о вреде жизни или здоровью, инспекторы вправе обойтись без предварительного уведомления. О плановой и внеплановой документарной проверке медорганизацию предупредят не меньше чем за три дня.

Срок проверок максимум 20 рабочих дней. Для медорганизации – субъекта малого предпринимательства длительность плановых выездных проверок – 50 часов в год для малого предприятия и 15 часов для микропредприятия.

Размеры штрафов

Инспекторы Роскомнадзора вправе выдавать предписания об устранении нарушений, составлять протоколы и направлять материалы в прокуратуру, подавать иски в суд, требовать заблокировать, уничтожить недостоверные или полученные незаконным путем персональные данные. Также накладывают штрафы. Какие и за что, посмотрите в таблице.

Штрафы юридических лиц за нарушение Закона о персональных данных

Вид нарушения	Штраф	Пояснения для главврача
Обработка персональных данных не соответствует заявленным целям	30 000—50 000 руб.	Иногда медорганизации перестраховываются. Просят пациентов дать согласие на обработку данных о семейном, имущественном положении, образовании, профессии, доходах и прочее. Если гражданин не подписывает документ, не оказывают медпомощь. Пациент не согласен предоставить личную информацию? Оцените, препятствует ли это оказанию медпомощи. Если нет, не отказывайте больному. Санкции проверяющих органов в таких случаях можно оспорить. Суды встают на сторону медорганизаций. Перечень сведений, которые нужно включить в согласие пациента на обработку персональных данных — в части 4 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Нет письменного согласия субъекта на обработку персональных данных	15 000—75 000 руб.	Письменное согласие брать нужно не всегда. Исключения — в части 2 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». В частности, если обработка персональных данных нужна для защиты жизни и здоровья человека, а получить его согласие невозможно. А вот биометрические данные можно обрабатывать только с письменного согласия (ст. 11). Это сведения о физиологических и биологических особенностях, на основании которых можно установить личность. Например, дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес, изображение человека. Рентгеновские и флюорографические снимки к биометрическим данным не относятся (разъяснения Роскомнадзора от 30.08.2013). Включать согласие на обработку персональных данных в договор с пациентом нельзя

Вид нарушения	Штраф	Пояснения для главврача
Медорганизация не разместила в открытом доступе документ, который определяет политику обработки персональных данных и требования к защите	15 000—30 000 руб.	Политика медорганизации по обработке и защите персональных данных должна распространяться на работников и пациентов (п. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»). Документ утверждает главврач
Пациенту не предоставили информацию об обработке персональных данных	20 000—40 000 руб.	Перечень сведений, которые вправе запросить пациент, — в части 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Медорганизация должна предоставить информацию в течение 30 дней с даты получения запроса (ч. 1 ст. 20)
Медорганизация не выполнила требования субъекта персональных данных	25 000—45 000 руб.	Пациент, чьи персональные данные обрабатывает медорганизация, может попросить уточнить неполные, устаревшие сведения. Выполнить запрос надо в течение 7 рабочих дней с даты получения (ч. 3 ст. 20, ч. 2 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»). При условии, что требования обоснованны. О принятых мерах надо уведомить пациента и третьих лиц, которым медорганизация передала его персональные данные
Медорганизация допустила несанкционированный доступ к персональным данным	25 000—50 000 руб.	Учреждения здравоохранения должны своевременно уточнять персональные данные. При необходимости блокировать или уничтожать. Проверьте меры защиты персональных данных. Достаточны ли они и насколько соответствуют требованиям нормативных актов. Положение об особенностях обработки персональных данных без использования средств автоматизации утверждено постановлением Правительства от 15.09.2008 № 687