



Министерство здравоохранения Нижегородской области
Государственное бюджетное учреждение здравоохранения
Нижегородской области
«Дзержинский психоневрологический диспансер»
(ГБУЗ НО «ДПНД»)

ПРИКАЗ

« 31 » декабря 2014 г. № 123
г. Дзержинск

**«Об утверждении политики в отношении обработки
персональных данных в ГБУЗ НО «ДПНД»**

В целях реализации Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказываю:

- Утвердить политику в отношении обработки персональных данных в ГБУЗ НО «ДПНД»;

Главный врач

М.А. Мартюшева

УТВЕРЖДАЮ

Главный врач

ГБУЗ НО «Дзержинский психоневрологический
диспансер»

М.А. Мартюшева

«11» октября 2014 г.

ПОЛИТИКА

в отношении обработки персональных данных в ГБУЗ НО «Дзержинский психоневрологический диспансер»

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) в ГБУЗ НО «Дзержинский психоневрологический диспансер» (далее – организация, оператор), разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

1.2. Целью Политики является реализация требований законодательства в области обработки и защиты персональных данных (далее – ПДн) и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн в организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.3. Обработка ПДн в организации осуществляется в связи с выполнением ею функций, предусмотренных ее учредительными документами, и определяемых:

- Федеральным законом от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановлением Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации.

Кроме того, обработка ПДн в организации осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых организация выступает в качестве работодателя (глава 14 Трудового кодекса Российской Федерации), в связи с реализацией организацией своих прав и обязанностей как юридического лица.

1.4. Политика вступает в силу с момента ее утверждения руководителем ГБУЗ НО «Дзержинский психоневрологический диспансер».

1.5. Политика подлежит пересмотру в ходе периодического анализа со стороны руководства учреждения, а также в случаях изменения законодательства Российской Федерации в области персональных данных.

2. ОСНОВНЫЕ ПОНЯТИЯ

2.1. Для целей Политики используются следующие понятия:

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

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;

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;

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

уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

3. ОБЛАСТЬ ДЕЙСТВИЯ

3.1. Положения Политики распространяются на все отношения, связанные с обработкой персональных данных, осуществляемой организацией:

- с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным;
- без использования средств автоматизации.

3.2. Политика применяется ко всем сотрудникам организации.

4. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Обработка персональных данных осуществляется организацией в следующих целях:

- обеспечение организации оказания медицинской помощи населению, а также наиболее полного исполнения обязательств и компетенций в соответствии с Федеральными законами от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан Российской Федерации», от 12 апреля 2010 г. № 61-ФЗ «Об обращении лекарственных средств» и от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании граждан в Российской Федерации», Правилами предоставления медицинскими организациями платных медицинских услуг, утвержденными Постановлением Правительства Российской Федерации от 4 октября 2012 г. № 1006;
- осуществление трудовых отношений;
- осуществление гражданско-правовых отношений.

5. КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В соответствии с целями обработки персональных данных, указанными в п.4 настоящей Политики, организацией осуществляется обработка следующих категорий субъектов персональных данных:

- физические лица, состоящие с организацией в трудовых отношениях;
- физические лица, являющиеся близкими родственниками сотрудников организации;
- физические лица, уволившиеся из организации;
- физические лица, являющиеся кандидатами на работу;
- физические лица, состоящие с организацией в гражданско-правовых отношениях;
- физические лица, обратившиеся в организацию для получения медицинской услуги.

5.2. Перечень обрабатываемых персональных данных утверждается нормативным актом учреждения.

6. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

6.2. Для обеспечения безопасности ПДн организация руководствуется следующими принципами:

- законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;
- системность: обработка ПДн в организации осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;
- комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах организации и других имеющихся в организации систем и средств защиты;
- непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;
- своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;
- преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн в организации с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;
- персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;
- минимизация прав доступа: доступ к ПДн предоставляется работникам только в объеме, необходимом для выполнения их должностных обязанностей;
- гибкость: обеспечение выполнения функций защиты ПДн при изменении характеристик функционирования информационных систем персональных данных организации, а также объема и состава обрабатываемых ПДн;
- специализация и профессионализм: реализация мер по обеспечению безопасности ПДн осуществляются работниками, имеющими необходимые для этого квалификацию и опыт;

- эффективность процедур отбора кадров: кадровая политика организации предусматривает тщательный подбор персонала и мотивацию работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн;
- наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;
- непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

6.3. В организации не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн в организации, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся организацией ПДн уничтожаются или обезличиваются.

6.4. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости – и актуальность по отношению к целям обработки. Организация принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

6.5. Условия обработки персональных данных

Условия обработки персональных данных, отличные от получения согласия субъекта персональных данных на обработку его персональных данных являются альтернативными.

6.5.1. Условия обработки специальных категорий персональных данных

Обработка специальных категорий персональных данных осуществляется организацией с соблюдением следующих условий:

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- обработка персональных данных 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 персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством;

– обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

– субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных.

6.5.2. Условия обработки биометрических персональных данных

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных организацией не обрабатываются.

6.5.3. Условия обработки общедоступных персональных данных

Обработка общедоступных персональных данных организацией не производится.

6.5.4. Поручение обработки персональных данных

6.5.4.1. Организация 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, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее – поручение).

6.5.4.2. Лицо, осуществляющее обработку персональных данных по поручению организации, соблюдает принципы и правила обработки персональных данных, предусмотренные настоящей Политикой. В поручении организации определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также указаны требования к защите обрабатываемых персональных данных.

6.5.4.3. При поручении обработки персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет организация. Лицо, осуществляющее обработку персональных данных по поручению организации, несет ответственность перед организацией.

6.6. Конфиденциальность персональных данных

6.6.1. Сотрудники организации, получившие доступ к персональным данным, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.7. Общедоступные источники персональных данных

6.7.1. Организация не создает общедоступные источники персональных данных.

6.8. Согласие субъекта персональных данных на обработку его персональных данных

6.8.1. При необходимости обеспечения условий обработки персональных данных

субъекта может предоставляться согласие субъекта персональных данных на обработку его персональных данных.

6.8.2. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. 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 организацией.

6.8.3. 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 выполнении альтернативных условий обработки персональных данных.

6.8.4. Обязанность представить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство выполнения альтернативных условий обработки персональных данных возлагается на организацию.

6.8.5. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. 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. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

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

3) наименование или фамилию, имя, отчество и адрес Оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;

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

9) подпись субъекта персональных данных.

6.8.6. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

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

6.8.8. 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.

6.8.9. Персональные данные могут быть получены организацией от лица, не являющегося субъектом персональных данных, при условии предоставления организации подтверждения наличия альтернативных условий обработки информации.

6.9. Трансграничная передача персональных данных

6.9.1. Трансграничная передача персональных данных учреждением не осуществляется.

6.10. Права субъектов персональных данных

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

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

- 1) подтверждение факта обработки персональных данных учреждением;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые учреждением способы обработки персональных данных;
- 4) наименование и место нахождения организации, сведения о лицах (за исключением работников организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с организацией 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 учреждения, если обработка поручена или будет поручена такому лицу;

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

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

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

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

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

– доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

– обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

6.10.1.3. Субъект персональных данных вправе требовать от организации 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.

6.10.1.4. Запрашиваемая субъектом информация должна быть предоставлена

субъекту персональных данных организацией 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.

6.10.1.5. Запрашиваемая информация предоставляется субъекту персональных данных или его представителю организацией 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 организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных организацией, подпись субъекта персональных данных или его представителя (далее – необходимая для запроса информация). Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

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

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

6.10.1.8. Организация вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на организации.

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

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

6.10.3. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

6.10.3.1. Принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, организацией не осуществляется.

6.10.4. Право на обжалование действий или бездействия Оператора

6.10.4.1. Если субъект персональных данных считает, что организация 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 организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

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

6.11. Обязанности Оператора

6.11.1. Обязанности Оператора при сборе персональных данных

6.11.1.1. При сборе персональных данных организация предоставляет субъекту персональных данных по его просьбе информацию, предусмотренную п.6.10.1.1. настоящей Политики.

6.11.1.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, организация разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

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

- 1) наименование либо фамилия, имя, отчество и адрес Оператора или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные Федеральным законом «О персональных данных» права субъекта персональных данных;
- 5) источник получения персональных данных.

6.11.1.4. Организация освобождается от обязанности предоставить субъекту Пдн сведения, предусмотренные п.6.11.1.3 в случаях, если:

- 1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных организацией;
- 2) персональные данные получены организацией на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- 3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- 4) организация осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
- 5) предоставление субъекту персональных данных информации, сообщаемой при получении персональных данных не от субъекта персональных данных, нарушает права и законные интересы третьих лиц.

6.11.2. Меры, направленные на обеспечение выполнения Оператором своих обязанностей

6.11.2.1. Организация принимает меры, необходимые и достаточные для обеспечения выполнения своих обязанностей. Организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, если иное не предусмотрено федеральными законами. К таким мерам, в частности, относятся:

- 1) назначение ответственного за организацию обработки персональных данных;
- 2) издание Политики, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных требованиям к защите персональных данных, Политике, локальным актам Оператора;
- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», соотношение указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;
- 6) ознакомление сотрудников организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, Политикой, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

6.11.3. Меры по обеспечению безопасности персональных данных при их обработке

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

6.11.3.2. Обеспечение безопасности персональных данных достигается, в частности:

- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) разработкой политики в отношении обработки персональных данных;
- 3) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных
- 4) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- 5) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- 6) учетом машинных носителей персональных данных;
- 7) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- 8) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 9) установлением правил доступа к Пдн, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с Пдн в информационной системе персональных данных;
- 10) применением сертифицированного антивирусного программного обеспечения с регулярно обновляемыми базами;
- 11) обучением работников организации непосредственно осуществляющих обработку персональных данных, положениям законодательства Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальным актам по вопросам обработки персональных данных;

- 12) контролем над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

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

6.11.4.1. Организация сообщает в установленном порядке субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

6.11.4.2. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя организация дает в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

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

6.11.4.4. Организация сообщает в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

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

6.11.5.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу

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

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

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

6.11.5.4. В случае достижения цели обработки персональных данных организация прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по ее поручению) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по ее поручению) 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 организацией и субъектом персональных данных, либо, если организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

6.11.5.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных организация прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по ее поручению) 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 ее поручению) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между организацией и субъектом персональных данных, либо, если организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

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

6.11.6. Уведомление об обработке персональных данных

6.11.6.1. Организация, за исключением случаев, предусмотренных Федеральным законом «О персональных данных», до начала обработки персональных данных уведомляет уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

6.11.6.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается уполномоченным лицом. Уведомление содержит следующие сведения:

- 1) наименование (фамилия, имя, отчество), адрес Оператора;
- 2) цель обработки персональных данных;
- 3) категории персональных данных;
- 4) категории субъектов, персональные данные которых обрабатываются;
- 5) правовое основание обработки персональных данных;
- 6) перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;

7) описание мер, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

8) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

9) дата начала обработки персональных данных;

10) срок или условие прекращения обработки персональных данных;

11) сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

12) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6.11.6.3. В случае изменения указанных сведений, а также в случае прекращения обработки персональных данных организация уведомляет об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

7. СФЕРЫ ОТВЕТСТВЕННОСТИ

7.1. Лица, ответственные за организацию обработки персональных данных в организации

7.1.1. Организация назначает лицо, ответственное за организацию обработки персональных данных.

7.1.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от исполнительного органа организации, являющейся Оператором, и подотчетно ему.

7.1.3. Организация предоставляет лицу, ответственному за организацию обработки персональных данных, сведения, предусмотренные п.6.11.6.2.

7.1.4. Лицо, ответственное за организацию обработки персональных данных, в частности, выполняет следующие функции:

1) осуществляет внутренний контроль за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2) доводит до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3) организывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов.

7.2. Ответственность

7.2.1. Лица, виновные в нарушении требований Федерального закона «О персональных данных», несут предусмотренную законодательством Российской Федерации ответственность.

7.2.2. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, установленных в соответствии с Федеральным законом «О персональных данных», подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8. КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

При достижении целей ожидаются следующие результаты:

- обеспечение защиты прав и свобод субъектов персональных данных при обработке его персональных данных учреждением;
- повышение общего уровня информационной безопасности учреждения;
- минимизация юридических рисков учреждения.