УТВЕРЖДАЮ
Директор ГОАПОУ «ЛКТиДХ»

_____ Р.В. Подмарков

«___» _____2023 г.

Правила обработки персональных данных

государственного областного автономного профессионального образовательного учреждения «Липецкий колледж транспорта и дорожного хозяйства»

Липецк 2023

Оглавление

1. Термины, определения и сокращения

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Автоматизированная система (АС) – Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Автоматизированное рабочее место (АРМ) – программно-технический комплекс АС, предназначенный для автоматизации деятельности определенного вида (Межгосударственный стандарт ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»).

Администратор безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Вспомогательные технические средства и системы (ВТСС) – технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, устанавливаемые совместно с основными техническими средствами и системами или в защищаемых помещениях (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Конфиденциальная информация - это определенные сведения, которые не подлежат без согласия их обладателя передаче и распространению лицом, получившим к ней доступ. (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Носитель защищаемой информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Носитель информации (НИ) – материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин ("Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утв. ФСТЭК РФ 15.02.2008)).

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Основные технические средства и системы (ОТСС) – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)).

Оператор персональных данных – 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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

Система защиты информации (СЗИ) – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для

защиты информации (Национальный стандарт Российской Федерации ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»).

Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу (Федеральный закон от 27.07.2006 № 152-ФЗ «О 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 (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»).

2. Назначение

2.1. Настоящие Правила обработки персональных данных в ГОАПОУ «ЛКТиДХ» (далее – Правила) имеют своей целью закрепление механизмов обеспечения прав субъекта на сохранение конфиденциальности информации о фактах, событиях и обстоятельствах его жизни, определяют основные требования к порядку сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачи), обезличивания, блокирования уничтожения (далее – обработки) персональных данных (далее – ПДн), а также права и обязанности работников ГОАПОУ «ЛКТиДХ» (далее – Организация) в области обработки ПДн.

2.2. В состав ПДн, обрабатываемых Организацией входят ПДн Субъектов, полученные от самих Субъектов ПДн или третьих лиц в рамках оказания государственных и муниципальных услуг, исполнения договоров, соглашений, и ПДн работников Организации:

– ПДн работника – информация, необходимая Организации для исполнения требований трудового законодательства и выполнения условий трудового договора с работником. ПДн работника содержатся в основных документах персонального учёта работников, хранящихся в личном деле работника, в информационных системах Организации и в других документах.

– ПДн Субъекта – информация, обрабатываемая Организацией в рамках исполнения требований и выполнения условий агентского договора, в рамках рассмотрения обращений граждан, а также в рамках предоставления государственных и муниципальных услуг. ПДн Субъекта содержатся в информационных системах Организации и/или на бумажном носителе.

2.3. Порядок Обработки ПДн определяется настоящими Правилами.

2.4. Данные Правила утверждаются и изменяются локальным нормативно-правовым актом Организации и действуют бессрочно.

3. Нормативные ссылки

Данные Правила разработаны с учетом требований следующих законодательных и нормативных актов:

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

– Федеральный закон от 27 июня 2006 № 152-ФЗ «О персональных данных»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства РФ от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным

законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Методический документ «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г.

– Информационное сообщение Федеральной службы по техническому и экспортному контролю от 30 июля 2012 г. N 240/24/3095 «Об утверждении требований к средствам антивирусной защиты»;

– Информационное сообщение Федеральной службы по техническому и экспортному контролю от 20 ноября 2012 г. N 240/24/4669 «Об особенностях защиты персональных данных при их обработке в информационных системах персональных данных и сертификации средств защиты информации, предназначенных для защиты персональных данных»;

– Информационное сообщение Федеральной службы по техническому и экспортному контролю от 15 июля 2013 г. N 240/22/2637 «По вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

4. Общие положения

4.1. Цели обработки персональных данных:

– обеспечение финансово-хозяйственной и иной деятельности учреждения, предусмотренной Уставом и действующим законодательством Российской Федерации;

– осуществление трудовых отношений с работниками и физическими лицами, намеревающимися вступить в трудовые отношения;

– осуществление функции оператора данных региональных информационных систем;

– оказание государственных и муниципальных услуг;

– исполнение договоров с партнерами учреждения.

4.2. Принципы обработки ПДн:

– обработка персональных данных осуществляется на законной и справедливой основе;

– обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

– не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только персональные данные, которые отвечают целям их обработки;

– содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не избыточны по отношению к заявленным целям их обработки;

– при обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает необходимые меры по уничтожению или уточнению неполных или неточных данных, либо обеспечивает их принятие;

– хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, ведомственными нормативно-правовыми актами, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.3. Правовое основание обработки персональных данных:

– Конституция Российской Федерации,
– Трудовой кодекс Российской Федерации,
– Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»,
– Федеральный закон от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации";
– Федеральный закон от 27.07.2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
– Устав ГОАПОУ «ЛКТиДХ».

5. Условия обработки персональных данных

5.1. Обработка ПДн Субъекта осуществляется в следующих случаях:

– с согласия Субъекта ПДн на обработку его персональных данных;

– для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Организацию функций, полномочий и обязанностей.

– в целях исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является Субъект ПДн, в том числе в случае реализации оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе Субъекта ПДн или договора, по которому Субъект ПДн будет являться выгодоприобретателем или поручителем;

– для исполнения полномочий федеральных органов исполнительной власти и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

5.2. Обработка ПДн осуществляется смешанным способом (как автоматизированная, так и неавтоматизированная обработка) путем сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачи), обезличивания, блокирования, уничтожения, а также осуществления иных действий с учетом требований действующего законодательства Российской Федерации. Полученная в ходе обработки ПДн информация может передаваться на бумажных носителях, электронных носителях, а также по

внутренней сети Организации, а также с использованием сети Интернет по защищенным каналам связи и доступна лишь строго определенному кругу лиц.

5.3. Организация обеспечивает конфиденциальность обрабатываемых ПДн. Сотрудники организации, связанные с получением, обработкой и защитой ПДн, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия Субъекта ПДн, если иное не предусмотрено действующим законодательством Российской Федерации.

6. Перечень участников процесса, их ответственность и функции

Участник процесса	Ответственность	Функции
Сотрудники, ответственные за ведение кадрового учета	1. Сохранение конфиденциальности ПДн работника и физических лиц, намеревающихся вступить в трудовые отношения с Организацией. 2. Получение согласия Субъекта ПДн на обработку его ПДн.	Обработка ПДн работника и физических лиц, намеревающихся вступить в трудовые отношения с Организацией
Работник	Своевременность и правильность предоставления своих ПДн	1. Предоставление своих ПДн ответственному работнику. 2. Уведомление ответственного работника об изменении своих ПДн.
Ответственный за организацию обработки персональных данных	1. Организация, координация и контроль деятельности Организации по обеспечению защиты ПДн. 2. Оказание структурным подразделениям Организации методической помощи по вопросам защиты ПДн.	1. Доведение до сведения сотрудников, допущенных к ПДн, положений законодательства РФ о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных; 2. Осуществление внутреннего контроля за соблюдением требований законодательства РФ и инструкций при обработке ПДн, в том числе требований к защите ПДн; 3. Организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов.
Администратор безопасности (системный администратор)	1. Обеспечение работоспособности элементов ИСПДн и средств защиты при обработке ПДн. 2. Обеспечение безопасности ПДн при их обработке в информационных системах ПДн. 3. Учет лиц, допущенных к работе с ПДн.	1. Организация доступа пользователей к защищаемым информационным и/или аппаратным ресурсам. 2. Выполнение требований по парольной защите. 3. Установка, настройка и сопровождение средств защиты информации, восстановление настроек средств защиты информации после сбоев. 4. Контроль за появлением новых версий программного обеспечения средств защиты. 5. Периодическое тестирование функций установленных средств защиты информации при изменении программной среды и/или полномочий пользователя.

Участник процесса	Ответственность	Функции
		6. Обеспечение целостности данных. 7. Обеспечение резервного копирования данных, восстановление информации, ПДн, уничтоженных вследствие несанкционированного доступа. 8. Анализ событий информационной безопасности, получаемых от средств защиты информации, а также обеспечение необходимых мер по устранению ситуаций нарушения информационной безопасности в будущем (оперативное реагирование на поступающие сигналы о нарушениях установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.). 9. Проведение расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению. При получении информации о возникновении вирусной активности (эпидемии) осуществляет информирование пользователей о возможной активности (эпидемии) и рекомендуемых действиях. 10. Сопровождение третьих лиц в помещения-места хранения носителей с защищаемой информацией и/или ПДн. 11. Организация обучения пользователей. 12. Организация учета, хранения и выдачи носителей с защищаемой информацией и/или ПДн. 13. Организация учета средств защиты информации, средств криптографической защиты информации, эксплуатационной и технической документации к ним. 14. Организация обмена информацией со сторонними организациями.
Пользователь ИСПДн	Соблюдение требований по режиму обработки ПДн.	1. Соблюдение требований по режиму обработки ПДн, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн; 2. Неразглашение ПДн, ставших ему известными вследствие исполнения им трудовых обязанностей; 3. Соблюдений требований парольной политики; 4. Соблюдения правил по работе в сетях общего доступа.

7. Получение Персональных данных

7.1. Получение Организацией ПДн Субъекта производится одним из ниже перечисленных способов:

7.1.1. Субъект ПДн непосредственно принимает решение о предоставлении ПДн и дает письменное согласие на их обработку Организацией. Форма Согласия субъекта на обработку ПДн представлена в Приложении №1 к настоящим Правилам (на примере согласия работника на

обработку ПДн). Форма Согласия на обработку персональных данных, разрешенных для распространения представлена в Приложении №2 к настоящим Правилам.

7.1.2. В случае недееспособности Субъекта ПДн согласие на обработку его ПДн дает законный представитель субъекта ПДн. В случае получения согласия на обработку ПДн от представителя Субъекта ПДн, полномочия данного представителя на дачу согласия от имени Субъекта ПДн должны проверяться Организацией.

7.1.3. В случае смерти Субъекта ПДн согласие на обработку его ПДн дают наследники Субъекта ПДн, если такое согласие не было дано Субъектом ПДн при его жизни.

7.1.4. ПДн так же могут быть получены от лица, не являющегося Субъектом ПДн, при условии наличия оснований для обработки ПДн из указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152 от 27 июля 2006 г. «О персональных данных». Например, письменное согласие Субъекта ПДн не требуется, если обработка ПДн осуществляется в целях исполнения договора, одной из сторон которого является Субъект ПДн.

7.2. Согласие на обработку ПДн может быть отозвано Субъектом ПДн или, в случае недееспособности Субъекта ПДн, законным представителем Субъекта ПДн. Форма отзыва согласия на обработку ПДн представлена в Приложении №3 к настоящим Правилам. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152 от 27 июля 2006 г. «О персональных данных».

7.3. Принятые ПДн подлежат учету, обработке и передаче в соответствии с нормами, установленными для ПДн, находящихся в Организации на постоянной основе.

8. Уточнение, хранение и уничтожение персональных данных

8.1. Хранение ПДн Субъектов осуществляется следующими способами:
- в бумажном виде;
- на машинных носителях, в том числе мобильных носителях;
- в информационных системах.

8.2. Сроки хранения ПДн

— ПДн Субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

— Документы, содержащие ПДн, подлежат хранению в порядке, предусмотренном архивным законодательством Российской Федерации.

— Срок хранения ПДн определяется в соответствии с Приказом Федерального архивного агентства от 20 декабря 2019 г. № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения», а также иными требованиями законодательства. Срок хранения различных категорий персональных данных приведен в Приложении №4 к настоящим Правилам.

8.3.Хранение ПДн в бумажном виде

8.3.1. Персональные данные Субъекта, представленные в бумажном виде, хранятся в подразделениях Организации, которые отвечают за взаимодействие с этим Субъектом или в учреждении, которому Организация поручила обработку ПДн.

8.3.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на

отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

8.3.3. При фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

8.3.4. Материальные носители ПДн, представленных в бумажном виде, должны храниться в сейфе, в запираемом металлическом шкафу или другим способом, исключающим несанкционированный доступ. Организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

8.4. Хранение ПДн на машинных носителях и в информационных системах

8.4.1. ПДн Субъекта, хранимые на машинных носителях, находятся в ведении подразделений Организации, осуществляющих эксплуатацию данных машинных носителей, используемых в информационной системе для хранения и обработки информации. Допуск к ПДн имеют работники Организации, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей.

8.4.2. В целях недопущения воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, организуется режим обеспечения безопасности помещений, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

8.4.3. Для обеспечения незамедлительного восстановления ПДн, хранимых на машинных носителях и в информационных системах, в случае несанкционированной модификации или уничтожения, необходимо выполнять процедуры регулярного резервного копирования, резервные копии должны храниться с исключением несанкционированного доступа к ним.

8.4.4. Машинные носители подлежат учету. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

8.4.5. Учет съемных машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства) информации ведется в журналах учета машинных носителей информации. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш- накопители, съемные жесткие диски).

8.4.6. Учет встроенных в портативные или стационарные технические средства машинных носителей информации (накопители на жестких дисках) может вестись в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

8.4.7. Регистрационные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета.

8.4.8. Руководителем Организации назначается должностное лицо (работник), ответственное за защиту информации (администратор безопасности).

8.5. Уточнение ПДн

8.5.1. В случае выявления неточных ПДн Организация обязана осуществить блокирование ПДн с момента такого выявления или получения запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта ПДн или третьих лиц.

Форма заявления Субъекта ПДн об изменении персональных данных представлена в Приложении №5 к настоящим Правилам.

8.5.2. 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.

8.5.3. Уточнение ПДн при осуществлении их обработки производится путем обновления или изменения данных на носителе. Если же это не допускается техническими особенностями носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн Субъекта.

8.6. Уничтожение ПДн

8.6.1. В случае выявления факта неправомерной обработки ПДн при обращении или по запросу Субъекта ПДн (его представителя или уполномоченного органа по защите прав субъектов персональных данных) Организация обязана уничтожить неправомерно обрабатываемые ПДн.

8.6.2. В случае выявления неправомерной обработки ПДн, осуществляемой Организацией или учреждением, действующим по поручению Организации, Организация в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку ПДн. В случае, если обеспечить правомерность обработки ПДн невозможно, Организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязана обеспечить уничтожение таких ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Организация уведомляет Субъект ПДн или его представителя, а в случае, если обращение Субъекта ПДн или его представителя было направлено уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

8.6.3. В случае достижения цели обработки ПДн Организация обеспечивает прекращение обработки ПДн и их уничтожение в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, иным соглашением между Организацией и Субъектом ПДн либо если Организация не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных федеральным законодательством. Форма Акта об уничтожении персональных данных субъекта персональных данных представлена в Приложении №6 к настоящим Правилам. Уничтожение персональных данных, содержащихся в информационных системах, дополнительно подтверждается выгрузкой из журнала регистрации событий информационной системы. Акт об уничтожении персональных данных и выгрузка из журнала регистрации событий информационной системы подлежат хранению в течение 3 лет с момента уничтожения ПДн.

8.6.4. В случае отзыва Субъектом ПДн согласия на обработку его ПДн Организация обеспечивает прекращение их обработки и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, обеспечивает уничтожение ПДн в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором или иным соглашением между Организацией и Субъектом ПДн либо если Организация не вправе осуществлять обработку ПДн без согласия Субъекта ПДн на основаниях, предусмотренных федеральным законодательством. Форма заявления Субъекта ПДн о прекращении обработки и уничтожении персональных данных представлена в Приложении №2 к настоящим Правилам.

8.6.5. Уничтожение персональных данных производится комиссией, состав которой утверждается локальным нормативно-правовым актом.

8.6.6. В случае отсутствия возможности уничтожения ПДн, оператор обязан произвести обезличивание этих ПДн.

8.6.7. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

8.6.8. Специализированными средствами или методами гарантированного уничтожения информации сотрудниками Организации обеспечивается уничтожение (стирание) информации на съемных и несъемных машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также производится контроль уничтожения (стирания) информации для исключения возможности восстановления защищаемой информации при передаче носителей.

9. Использование Персональных данных Субъекта

9.1. Допуск к ПДн Субъекта имеют работники Организации, которым ПДн необходимы в связи с исполнением ими трудовых обязанностей.

9.2. Лица, ответственные за организацию обработки ПДн, утверждены приказом по Организации.

9.3. Лица, осуществляющие обработку ПДн (в том числе сотрудники Организации или лица, осуществляющие такую обработку по поручению), информируются о факте обработки ими ПДн, категории обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Организации.

9.4. Допуск работника к обработке ПДн должен осуществляться только после ознакомления с внутренними нормативными актами Организации, определяющими порядок обработки и защиты ПДн с использованием и без использования средств автоматизации.

9.5. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны не раскрывать третьим лицам и не распространять ПДн без согласия Субъекта ПДн, если иное не предусмотрено федеральными законами.

9.6. Сотрудники обязаны подписать соглашение о неразглашении ПДн. Форма соглашения о неразглашении ПДн представлена в Приложении №8 настоящих Правил.

10. Передача Персональных данных Субъекта третьим лицам

10.1. Передача ПДн Субъекта третьим лицам осуществляется только с согласия Субъекта ПДн.

10.2. Согласия Субъекта на передачу его ПДн третьим лицам не требуется в случаях:

10.2.1. когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта;

10.2.2. когда согласие Субъекта на передачу его ПДн третьим лицам получено от него в письменном виде при заключении договора с Организацией;

10.2.3. когда третьи лица оказывают услуги Организации на основании заключенных договоров;

10.2.4. а также в случаях, установленных федеральными законами и настоящими Правилами.

10.3. Персональные данные Субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого Субъекта, за исключением случаев, когда передача ПДн Субъекта без его согласия допускается действующим законодательством РФ.

10.4. Предоставление ПДн Субъекта государственным органам производится в соответствии с требованиями действующего законодательства.

10.4.1. При поступлении запроса из уполномоченного органа по защите прав субъектов персональных данных запрос регистрируется в Журнале регистрации входящей корреспонденции Организации.

10.4.2. Зарегистрированный запрос уполномоченного органа по защите прав субъектов персональных данных передается лицу, ответственному за обработку ПДн. Ответственное лицо обязано:

– Осуществлять подготовку документов в соответствии с перечнем и в сроки, указанные в запросе уполномоченного органа по защите прав субъектов персональных данных;

– В случае затребования оригиналов документов организовать подготовку описи передачи документов;

– При дополнительных запросах требующихся документов, предоставить их в указанные сроки.

11. Защита персональных данных

11.1. Защита ПДн обеспечивается на всех стадиях (этапах) их обработки.

11.2. Организационные и технические меры защиты ПДн направлены на исключение:

11.2.1. неправомерных доступа, копирования, предоставления или распространения (обеспечение конфиденциальности информации);

11.2.2. неправомерных уничтожения или модифицирования (обеспечение целостности информации);

11.2.3. неправомерного блокирования (обеспечение доступности информации).

11.3. Для обеспечения защиты ПДн, содержащихся в информационной системе, проводятся следующие мероприятия:

11.3.1. формирование требований к защите ПДн, содержащихся в информационной системе;

11.3.2. разработка системы защиты информационной системы, включающей комплекс организационных и технических мер защиты;

11.3.3. внедрение системы защиты информационной системы;

11.3.4. аттестация информационной системы по требованиям безопасности информации и ввод ее в действие;

11.3.5. обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы.

11.4. Меры защиты информации реализуются в информационной системе в рамках ее системы защиты в зависимости от уровня защищенности персональных данных в информационной системе, актуальных угроз безопасности информации, структурно-функциональных характеристик информационной системы, применяемых информационных технологий и особенностей функционирования информационной системы. В информационной системе подлежат реализации следующие меры защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- обеспечение доступности информации;
- защита технических средств;
- защита информационной системы, ее средств и систем связи и передачи данных.

11.5. Содержание мер защиты информации для их реализации в информационных системах Организации приведено в технической документации информационной системы.

12. Права и обязанности субъектов персональных данных

12.1. В целях обеспечения защиты ПДн Субъекты имеют право:

– получать полную информацию о своих ПДн и их обработке (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим ПДн, включая право получать копии любой записи, содержащей ПДн Субъекта, за исключением случаев, предусмотренных федеральным законом;

– требовать исключения или исправления неверных или неполных ПДн, а также данных, обработанных с нарушением законодательства;

– при отказе Организации или уполномоченного им лица исключить или исправить ПДн Субъекта – заявить в письменной форме о своем несогласии, представив соответствующее обоснование;

– потребовать от Организации или уполномоченного им лица уведомления всех лиц, которым ранее были сообщены неверные или неполные ПДн субъекта, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать в суд любые неправомерные действия или бездействие Организации или уполномоченного им лица при обработке и защите ПДн Субъекта.

12.2. Субъект ПДн или его законный представитель обязуется предоставлять ПДн, соответствующие действительности.

13. Ответственность

13.1. Руководитель, разрешающий доступ сотрудника к документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

13.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

14. Актуализация

14.1. Решение об изменении документа принимает ответственный за организацию обработки персональных данных, назначенный приказом Руководителя Организации, на основании предложений других подразделений, результатов применения документа в Организации, анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних аудитов.

Председатель ПДТК  О.Б. Иванилова