ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00CE6439D909A541A05A096BEB9AAA1F99
Владелец: Нижник Евгений Алексеевич
Действителен: с 25.11.2025 до 18.02.2027

«УТВЕРЖДЕНО»

Ректор ФГБОУ ВО АГПУ

_____Нижник Е.А.

«____» _____ 2026 г.

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «АРМАВИРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

П-1-29-10-26

Армавир, 2026 г.

ПОЯСНЕНИЕ К РЕДАКЦИИ 2026 ГОДА

Настоящая редакция подготовлена на основе Положения об обработке и защите персональных данных в ФГБОУ ВО «АГПУ» (СМК-П-1-14-05-2021), утверждённого 27.05.2021. Основные разделы, определения и структура сохранены. Изменения обусловлены поправками в законодательство Российской Федерации о персональных данных (далее - ПДн), вступившими в силу в период 2022–2026 годов. В августе 2026 г. в раздел 4 внесено дополнение (пункт 4.5) о разделении функций исполнения и внутреннего контроля (надзора) за обеспечением информационной безопасности.

Основания для внесения изменений:

• Федеральный закон от 14.07.2022 № 266-ФЗ — введение обязанности уведомления Роскомнадзора об утечках ПДн, изменения в порядке трансграничной передачи, изменения в требованиях к согласию;

• Федеральный закон от 29.12.2022 № 572-ФЗ — особый режим обработки биометрических персональных данных;

• Федеральный закон от 30.11.2024 № 420-ФЗ — введение оборотных штрафов и увеличение ответственности за нарушения в области ПДн (с 30.05.2026);

• Приказ Роскомнадзора от 27.10.2022 № 178 — требования к оценке вреда, который может быть причинён субъектам ПДн;

• Приказ Роскомнадзора от 28.10.2022 № 179 — требования к подтверждению уничтожения ПДн (действует с 01.03.2023 по 01.03.2029);

• Приказ ФСТЭК России от 11.04.2025 № 117 — новые требования к защите информации в информационных системах государственных учреждений (с 01.03.2026, заменил Приказ № 17).

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке и защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Армавирский государственный педагогический университет» (далее – Положение) разработано в соответствии с:

– Трудовым кодексом Российской Федерации;

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (в действующей редакции; далее – Федеральный закон № 152-ФЗ);

– Федеральным законом от 14.07.2022 № 266-ФЗ (в части введения обязанности уведомления об утечках персональных данных, изменений в порядке трансграничной передачи);

– Федеральным законом от 29.12.2022 № 572-ФЗ (в части обработки биометрических персональных данных);

– Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказом 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»;

– Приказом ФСБ России от 10.07.2014 № 378 (в отношении мер защиты ПДн с использованием средств криптографической защиты информации);

– Приказом Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда…»;

– Приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

– иными нормативными правовыми актами в области персональных данных;

– локальными нормативными актами федерального государственного бюджетного образовательного учреждения высшего образования «Армавирский государственный педагогический университет» (далее – ФГБОУ ВО «АГПУ», АГПУ, университет).

1.2. Настоящее Положение принято с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Настоящее Положение определяет политику университета в отношении обработки персональных данных, требования к их защите и порядок реализации мер, направленных на обеспечение выполнения обязанностей оператора персональных данных.

2. ОСНОВНЫЕ ПОНЯТИЯ, ИСПОЛЬЗУЕМЫЕ В ПОЛОЖЕНИИ

2.1. В целях настоящего Положения используются следующие основные понятия:

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

2) **персональные данные, разрешённые субъектом персональных данных для распространения** – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путём дачи согласия на обработку персональных данных, разрешённых субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом № 152-ФЗ;

3) **специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, а также сведения о судимости;

4) **биометрические персональные данные** – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;

5) **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, в том числе ФГБОУ ВО «АГПУ»;

6) **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;

7) **автоматизированная обработка персональных данных** – обработка персональных данных с помощью средств вычислительной техники;

8) **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределённому кругу лиц;

9) **предоставление персональных данных** – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

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

11) **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;

12) **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность

персональных данных конкретному субъекту персональных данных;

13) **информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

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

15) **инцидент, связанный с обработкой персональных данных** – неправомерная или случайная передача (предоставление, распространение, доступ) персональных данных, повлёкшая нарушение прав субъектов персональных данных;

3. ОСНОВНЫЕ УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, полученного в форме, установленной Федеральным законом № 152-ФЗ, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

3.2. Согласие на обработку персональных данных, разрешённых субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешённых субъектом персональных данных для распространения, в соответствии с требованиями к составу такого согласия, установленными Приказом Роскомнадзора от 24.02.2021 № 18.

3.2.1. Согласие на обработку биометрических персональных данных оформляется в письменной форме или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью субъекта персональных данных, отдельно от иных согласий. В согласии указывается цель обработки и информация о том, размещаются ли биометрические персональные данные в единой биометрической системе. При использовании биометрических персональных данных для идентификации личности оператор обеспечивает их размещение исключительно в Единой биометрической системе в соответствии с требованиями Федерального закона от 29.12.2022 № 572-ФЗ.

3.2.2. Обработка специальных категорий персональных данных (сведений о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, судимости) допускается только в случаях, предусмотренных частью 2 статьи 10 Федерального закона № 152-ФЗ, в том числе при наличии письменного согласия субъекта персональных данных.

3.3. Передача (распространение, предоставление, доступ) персональных данных, разрешённых субъектом персональных данных для распространения, должна быть прекращена в любое время по требованию субъекта персональных данных. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных

данных, а также перечень персональных данных, обработка которых подлежит прекращению. Указанные в данном требовании персональные данные могут обрабатываться только оператором, которому оно направлено.

3.4. Оператор осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

3.5. Допуск работников университета к обработке персональных данных осуществляется на основании приказа (распорядительного акта) ФГБОУ ВО «АГПУ».

3.6. Обработка персональных данных осуществляется путём:

1) получения персональных данных в устной и письменной форме непосредственно с согласия субъекта персональных данных на обработку его персональных данных;

2) внесения персональных данных в документы, реестры и информационные системы оператора;

3) использования иных способов обработки персональных данных, не противоречащих Федеральному закону № 152-ФЗ.

3.7. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3.8. Передача персональных данных органам судебной власти, правоохранительным органам, в органы Федеральной налоговой службы, Фонда пенсионного и социального страхования Российской Федерации, в другие уполномоченные органы и организации осуществляется в соответствии с требованиями законодательства Российской Федерации.

3.9. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обеспечивает 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 в части 5 статьи 18 Федерального закона № 152-ФЗ.

3.10. Цели обработки персональных данных:

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

3.10.2. Обработка оператором персональных данных осуществляется в следующих целях:

1) обеспечение соблюдения Конституции Российской Федерации, федеральных законов, иных нормативных правовых актов, локальных нормативных актов университета;

2) осуществление деятельности в соответствии с уставом ФГБОУ ВО «АГПУ», видами экономической деятельности университета по Общероссийскому классификатору видов экономической деятельности, включёнными в Единый государственный реестр юридических лиц;

3) ведение кадрового делопроизводства;

4) содействие работникам в трудоустройстве, получении образования и продвижении по службе, обеспечение личной безопасности работников, контроль количества и качества

выполняемой работы, обеспечение сохранности имущества;

5) привлечение и отбор кандидатов на работу у оператора;

6) организация постановки на индивидуальный (персонифицированный) учёт работников в системе обязательного пенсионного страхования;

7) заполнение и передача в органы исполнительной власти и иные уполномоченные органы и организации требуемых форм отчётности;

8) осуществление гражданско-правовых отношений;

9) ведение бухгалтерского учёта;

10) осуществление пропускного режима;

11) организация приёма на обучение (прохождение приёмной кампании);

12) реализация образовательных программ, проведение учебного процесса, промежуточной и итоговой аттестации;

13) выполнение обязанностей университета в отношении федеральных информационных систем (ФИС ФРДО, суперсервис «Поступление в вуз онлайн», иных государственных информационных систем в области образования);

14) обеспечение проведения научной и научно-исследовательской деятельности;

15) организация воспитательной работы и молодёжной политики;

16) обеспечение функционирования системы контроля и управления доступом, системы видеонаблюдения на объектах университета.

3.11. Категории субъектов персональных данных, обработка персональных данных которых осуществляется оператором:

1) физические лица, поступающие на обучение (абитуриенты);

2) обучающиеся;

3) физические лица, поступающие на работу;

4) работники;

5) физические лица, обработка персональных данных которых необходима для исполнения договора (контракта, соглашения), стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора (контракта, соглашения) по инициативе субъекта персональных данных или договора (контракта, соглашения), по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

6) иные физические лица, обработка персональных данных которых необходима для исполнения законодательства Российской Федерации и (или) локальных нормативных актов университета;

7) физические лица, являющиеся представителями (законными представителями) вышеперечисленных категорий субъектов персональных данных.

3.12. Хранение персональных данных.

3.12.1. Оператор осуществляет хранение персональных данных 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, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.12.2. Персональные данные могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

3.12.3. Персональные данные, зафиксированные на бумажных носителях, хранятся в запираемых шкафах либо в запираемых помещениях с ограниченным правом доступа.

3.12.4. Персональные данные, полученные в электронном виде, хранятся на электронных носителях, доступ к которым имеют только уполномоченные оператором лица.

3.12.5. Персональные данные, разрешённые субъектом персональных данных для распространения в соответствии с Федеральным законом № 152-ФЗ, могут размещаться в местах с доступом неограниченного круга лиц.

3.13. Трансграничная передача персональных данных.

3.13.1. До начала осуществления трансграничной передачи персональных данных оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своём намерении осуществлять трансграничную передачу персональных данных в порядке, установленном частями 3–7 статьи 12 Федерального закона № 152-ФЗ.

3.13.2. Трансграничная передача персональных данных на территории иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных (перечень утверждается Роскомнадзором), осуществляется в общем порядке.

3.13.3. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, допускается только при наличии оснований, предусмотренных частью 4 статьи 12 Федерального закона № 152-ФЗ, в том числе при наличии письменного согласия субъекта персональных данных на трансграничную передачу его персональных данных с указанием получателя и целей передачи.

3.14. Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

3.15. Отзыв согласия на обработку персональных данных может быть осуществлён субъектом персональных данных в любой форме, позволяющей надёжно идентифицировать его личность. В целях ускорения обработки обращений субъектам персональных данных рекомендуется использовать Типовую форму заявления на отзыв согласия, размещённую на официальном сайте Университета.

Направление отзыва может быть реализовано следующими способами:

1) путём подачи письменного заявления оператору лично или направления его почтовой связью;

2) путём подачи заявления в электронной форме, подписанного усиленной квалифицированной электронной подписью;

3) иными способами, обеспечивающими однозначную идентификацию субъекта персональных данных».

3.16. Оператор обязан прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению

оператора:

1) в случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, в срок, не превышающий трёх рабочих дней с даты этого выявления;

2) в случае отзыва субъектом персональных данных согласия на обработку его персональных данных — не позднее 30 дней с даты получения отзыва (если иное не предусмотрено законодательством);

3) в случае достижения цели обработки персональных данных — не позднее 30 дней с даты достижения цели.

3.17. Уничтожение персональных данных.

3.17.1. Уничтожение персональных данных производится способами, обеспечивающими невозможность восстановления содержания персональных данных: путём сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок (для бумажных носителей); путём стирания или форматирования (для электронных носителей); иными способами, в результате которых становится невозможным восстановление персональных данных.

3.17.2. Факт уничтожения персональных данных подтверждается документально в соответствии с Приказом Роскомнадзора от 28.10.2022 № 179:

1) при обработке персональных данных без использования средств автоматизации — актом об уничтожении персональных данных;

2) при обработке персональных данных с использованием средств автоматизации — актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных.

3.17.3. Акт об уничтожении персональных данных должен содержать сведения, установленные пунктами 3–4 Приказа Роскомнадзора от 28.10.2022 № 179, включая: наименование оператора и его адрес; фамилию, имя, отчество субъекта персональных данных; фамилию, имя, отчество, должность и подпись лиц, уничтоживших персональные данные; перечень категорий уничтоженных персональных данных; наименование материального носителя или информационной системы; способ уничтожения; дату уничтожения.

3.17.4. Акт об уничтожении персональных данных составляется на бумажном носителе с личной подписью или в электронном виде с усиленной квалифицированной электронной подписью лиц, осуществивших уничтожение.

3.17.5. Форма акта об уничтожении персональных данных утверждается отдельным приказом ректора университета.

4. ОСНОВНЫЕ ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Оператор 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, в том

числе:

1) определяет угрозы безопасности персональных данных при их обработке, включая угрозы, связанные с компьютерными атаками, и разрабатывает (актуализирует) модели угроз безопасности информации в соответствии с методикой ФСТЭК России от 05.02.2021 и Приказом ФСТЭК России от 11.04.2025 № 117;

2) принимает локальные нормативные акты и иные документы, регулирующие отношения в сфере обработки и защиты персональных данных;

3) обеспечивает пропускной режим в ФГБОУ ВО «АГПУ» и охрану территории, зданий, помещений университета;

4) определяет лиц, допущенных к обработке персональных данных;

5) определяет лиц, ответственных за обеспечение безопасности (защиты) персональных данных, а также лицо, ответственное за организацию обработки персональных данных (в соответствии со статьёй 22.1 Федерального закона № 152-ФЗ);

6) создаёт необходимые условия для обработки персональных данных, при которых обеспечивается их сохранность и исключается несанкционированный доступ к ним;

7) организует учёт машинных носителей персональных данных;

8) организует работу с информационными системами, в которых обрабатываются персональные данные, в том числе путём установки индивидуальных паролей доступа в указанные информационные системы;

9) применяет прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации (в соответствии с Приказом ФСТЭК России от 18.02.2013 № 21 и Приказом ФСТЭК России от 11.04.2025 № 117);

10) проводит мероприятия по выявлению (обнаружению) фактов несанкционированного доступа к персональным данным и принимает соответствующие меры;

11) осуществляет восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

12) обеспечивает уничтожение либо обезличивание персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом;

13) осуществляет контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных;

14) осуществляет оценку вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, в порядке, установленном Приказом Роскомнадзора от 27.10.2022 № 178;

15) обеспечивает уведомление уполномоченного органа по защите прав субъектов персональных данных о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлёкших нарушение прав субъектов персональных данных, в порядке и сроки, установленные частью 3.1 статьи 21 Федерального закона № 152-ФЗ.

4.2. Порядок реагирования на инциденты, связанные с обработкой персональных данных.

4.2.1. При выявлении признаков нарушения безопасности персональных данных работники Университета обязаны незамедлительно сообщить об этом в порядке, установленном Регламентом реагирования на инциденты информационной безопасности Университета.

Выявленные признаки инцидента подлежат регистрации и предварительной оценке. Университет организует принятие необходимых мер по предотвращению или ограничению возможных негативных последствий, установлению обстоятельств произошедшего и устранению выявленных нарушений.

4.2.2. При установлении факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлёкшей нарушение прав субъектов персональных данных, Университет в соответствии с частью 3.1 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязан уведомить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор):

— в течение 24 часов с момента выявления инцидента — о произошедшем инциденте, предполагаемых причинах, повлёкших нарушение прав субъектов персональных данных, предполагаемом вреде, причинённом правам субъектов персональных данных, принятых мерах по устранению последствий инцидента, а также предоставить сведения о лице, уполномоченном Университетом на взаимодействие с Роскомнадзором по вопросам указанного инцидента;

— в течение 72 часов с момента выявления инцидента — о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной инцидента (при наличии).

Исчисление указанных сроков осуществляется с момента выявления инцидента Университетом, Роскомнадзором или иным лицом в соответствии с законодательством Российской Федерации.

4.2.3. Подготовка и направление уведомлений в Роскомнадзор осуществляются в порядке, установленном законодательством Российской Федерации, с использованием предусмотренных для этого форм и способов направления уведомлений.

Организацию выполнения требований настоящего раздела обеспечивает лицо, ответственное за организацию обработки персональных данных в Университете.

Непосредственное выполнение мероприятий по анализу инцидента, подготовке необходимых сведений и направлению уведомлений возлагается на уполномоченных должностных лиц Университета в соответствии с установленным распределением обязанностей.

4.2.4. Порядок выявления, регистрации, оценки и расследования инцидентов, взаимодействия структурных подразделений и ответственных должностных лиц, подготовки и направления уведомлений в уполномоченные государственные органы, а также осуществления мероприятий по устранению последствий инцидентов определяется Регламентом реагирования на инциденты информационной безопасности Университета.

При выполнении указанных мероприятий Университет обеспечивает соблюдение установленных законодательством Российской Федерации требований и сроков.

4.3. Оценка вреда, который может быть причинён субъектам персональных данных.

4.3.1. ФГБОУ ВО «АГПУ» осуществляет оценку вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, в порядке, установленном Приказом Роскомнадзора от 27.10.2022 № 178.

4.3.2. Оценка вреда проводится в отношении каждой информационной системы персональных данных и (или) каждой цели обработки персональных данных и оформляется актом.

4.3.3. Оценка вреда пересматривается не реже одного раза в три года, а также в случае изменения условий обработки, состава обрабатываемых персональных данных, категорий субъектов персональных данных, применяемых мер защиты информации.

4.4. Уведомление уполномоченного органа об обработке персональных данных.

4.4.1. ФГБОУ ВО «АГПУ» направляет в Роскомнадзор уведомление о своём намерении осуществлять обработку персональных данных в порядке, установленном статьёй 22 Федерального закона № 152-ФЗ.

4.4.2. Оператор обязан своевременно (в течение 10 рабочих дней с момента наступления изменений) уведомлять Роскомнадзор об изменении сведений, указанных в уведомлении об обработке персональных данных.

4.4.3. Уведомления направляются в электронной форме через личный кабинет оператора на сайте pd.rkn.gov.ru либо на бумажном носителе.

4.5. Внутренний контроль (надзор) за обеспечением информационной безопасности и защиты персональных данных.

4.5.1. В целях обеспечения выполнения обязанности, предусмотренной пунктом 4 части 1 статьи 18.1 Федерального закона № 152-ФЗ, в Университете реализована модель разделения функций исполнения и контроля: организационные и технические меры защиты персональных данных реализуются структурными подразделениями Университета и ответственным за информационно-техническую инфраструктуру, а контроль за их выполнением осуществляет главный специалист по защите информации, наделённый функциями органа внутреннего контроля (надзора).

4.5.2. Полномочия главного специалиста по защите информации, порядок проведения проверок структурных подразделений, формы актов проверок и предписаний об устранении нарушений устанавливаются приказом ректора университета об организации работы по обработке и защите персональных данных и обеспечению информационной безопасности.

4.5.3. Главный специалист по защите информации не несёт ответственности за непосредственное исполнение организационных и технических мер защиты персональных данных структурными подразделениями Университета. Ответственность за фактическое исполнение таких мер несут руководители соответствующих структурных подразделений и ответственный за информационно-техническую инфраструктуру.

5. ОСНОВНЫЕ ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. 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 № 152-ФЗ;

8) информацию об осуществлённой или о предполагаемой трансграничной передаче персональных 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 № 152-ФЗ или другими федеральными законами.

5.2. 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.

5.3. Субъект персональных данных вправе отозвать своё согласие на обработку персональных данных в любой форме, позволяющей идентифицировать субъекта персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных только при наличии оснований, предусмотренных Федеральным законом № 152-ФЗ.

5.4. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ 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.

5.5. В случае предоставления персональных данных для обработки, субъект персональных данных (его законный представитель, представитель) обязан предоставлять оператору только достоверные персональные данные.

6. ОСНОВНЫЕ ОБЯЗАННОСТИ И ПРАВА ОПЕРАТОРА

6.1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона № 152-ФЗ.

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

6.3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона № 152-ФЗ, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию: наименование либо фамилия, имя, отчество и адрес оператора или его представителя; цель обработки персональных данных и её правовое основание; предполагаемые пользователи персональных данных; установленные Федеральным законом № 152-ФЗ права субъекта персональных данных; источник получения персональных данных.

6.4. Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам, в частности, относятся:

1) назначение оператором ответственного за организацию обработки персональных данных (в соответствии со статьёй 22.1 Федерального закона № 152-ФЗ);

2) издание оператором документов, определяющих политику оператора в отношении обработки персональных данных, 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 в соответствии со статьёй 19 Федерального закона № 152-ФЗ;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

7) опубликование или иное обеспечение неограниченного доступа к политике оператора в отношении обработки персональных данных;

8) уведомление уполномоченного органа по защите прав субъектов персональных данных о своём намерении осуществлять обработку персональных данных, а также о случаях выявления инцидентов, связанных с обработкой персональных данных, в порядке, установленном Федеральным законом № 152-ФЗ.

6.5. Оператор персональных данных вправе:

1) отстаивать свои интересы законными способами, в том числе путём обращения в суд;

2) предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);

3) отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;

4) использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Лица, ответственные за организацию обработки персональных данных и (или) их защиту, а также лица, допущенные в установленном порядке к обработке персональных данных, виновные в нарушении требований Федерального закона № 152-ФЗ, в том числе в случае нарушения конфиденциальности персональных данных, несут предусмотренную законодательством Российской Федерации ответственность:

– дисциплинарную;

– административную;

– гражданско-правовую;

– уголовную.

7.2. Административная ответственность за нарушения в сфере персональных данных установлена статьёй 13.11 Кодекса Российской Федерации об административных правонарушениях (в редакции Федерального закона от 30.11.2024 № 420-ФЗ, действующей с 30.05.2026). За утечку персональных данных, в зависимости от объёма и категории данных, размер штрафа для юридического лица составляет от 3 до 20 миллионов рублей; за повторную утечку — от 1 до 3 процентов совокупной годовой выручки, но не менее 20 миллионов и не более 500 миллионов рублей.

7.3. Субъект персональных данных (его законный представитель, представитель), предоставивший оператору заведомо недостоверные сведения о своих (субъекта) персональных данных, несёт юридическую ответственность в соответствии с законодательством Российской Федерации.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение вступает в силу с даты утверждения его Ученым советом Университета и обязательно для исполнения всеми структурными подразделениями.

8.2. Изменения и дополнения вносятся в том же порядке, в котором утверждалось Положение.

8.3. Со дня введения в действие настоящего Положения признать утратившими силу:

– Положение об обработке и защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Армавирский государственный педагогический университет» (СМК-П-1-14-05-2021), утверждённое приказом ФГБОУ ВО «АГПУ» от 27.05.2021 № 71.

8.3. Актуальная редакция настоящего Положения размещается на официальном сайте университета в информационно-телекоммуникационной сети «Интернет» и доступна для ознакомления работникам и иным заинтересованным лицам.