	Министерство просвещения Российской Федерации
	Федеральное государственное бюджетное образовательное учреждение высшего образования «Армавирский государственный педагогический университет»
П-1-29-10-26	Локальные нормативные акты, регламентирующие общие положения
	Регламент организации работы с персональными данными в структурных подразделениях и служебных помещениях в федеральном государственном бюджетном образовательном учреждении высшего образования «Армавирский государственный педагогический университет»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

«УТВЕРЖДАЮ»
Ректор ФГБОУ ВО «АГПУ»
_____ Е.А. Нижник
«____» _____ 2026 г.

РЕГЛАМЕНТ ОРГАНИЗАЦИИ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЯХ И СЛУЖЕБНЫХ ПОМЕЩЕНИЯХ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ «АРМАВИРСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Р-1-31-10-26

Армавир, 2026

Рассмотрен ППО работников и обучающихся ФГБОУ ВО «АГПУ» общероссийского Профсоюза образования	*Протокол №13 от «16» октября 2026 г.*
Рассмотрен студенческим советом ФГБОУ ВО «АГПУ»	*Протокол № 2 от «13» октября 2026 г.*
Рассмотрен советом родителей (законных представителей) несовершеннолетних обучающихся ФГБОУ ВО «АГПУ»	*Протокол № 2 от «14» октября 2026 г.*
Принят (утвержден) ученым советом ФГБОУ ВО «АГПУ»	*Протокол № 18 от «23» октября 2026г.*
Регистрационный номер по журналу учета, дата регистрации	*№ 31 от «23» октября 2026г.*
Р-1-31-10-26	Стр. 1 из 22

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент определяет обязательный для работников ФГБОУ ВО «АГПУ» (далее — Университет) порядок работы с персональными данными (далее — ПДн), требования к рабочим местам, правила обращения с носителями информации, разграничение обязанностей и порядок контроля.

1.2. Университет является оператором ПДн в соответствии с ФЗ № 152-ФЗ. Работники Университета, допущенные к обработке ПДн, не становятся самостоятельными операторами и несут персональную ответственность за выполнение своих обязанностей.

1.3. Регламент обязателен для выполнения при обработке ПДн всех категорий субъектов (сотрудников, обучающихся, поступающих, контрагентов и др.) как с использованием средств автоматизации, так и без них, включая работу в помещениях Университета и в дистанционном режиме.

1.4. Регламент применяется совместно с иными локальными нормативными актами Университета в сфере информационной безопасности и защиты ПДн. В случае противоречий между ними приоритет имеют нормы федерального законодательства.

1.5. Правовую основу Регламента составляют: Трудовой кодекс РФ, Федеральные законы № 152-ФЗ и № 149-ФЗ, Постановления Правительства РФ № 687 и № 1119, нормативные акты ФСТЭК России и Роскомнадзора.

1.6. Организационные и технические меры защиты определяются Университетом исходя из характера ПДн, объема обработки и актуальных рисков. Запрещается избыточное дублирование учетных форм и документов, содержащих ПДн.

1.7. Зонирование помещений Университета применяется исключительно для разграничения прав доступа сотрудников и не связано с категорированием объектов критической информационной инфраструктуры.

2. ТЕРМИНЫ, ЦЕЛИ ОБРАБОТКИ И ОРГАНИЗАЦИЯ ДОСТУПА

2.1. ПДн — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу. Обработка ПДн охватывает получение, сбор, запись, систематизацию, хранение, уточнение, использование, передачу, обезличивание, блокирование, удаление и уничтожение в значении статьи 3 Закона № 152-ФЗ.

2.2. Уполномоченный работник (исполнитель обработки) — работник, допущенный к конкретным категориям ПДн для исполнения должностных обязанностей. Ответственный за организацию обработки ПДн — лицо, назначенное приказом ректора по статье 22.1 Закона № 152-ФЗ. Руководитель подразделения — лицо, организующее конкретный процесс обработки и режим закреплённых помещений.

2.3. При работе с ПДн различаются помещения для приёма посетителей, служебные рабочие места, места хранения бумажных дел и технические помещения. Их фактический режим определяется выполняемыми функциями и риском доступа посторонних. Обязательного присвоения буквенных категорий, маркировки зон или выделения отдельной комнаты для каждого вида обработки настоящий Регламент не требует.

2.4. В одном кабинете могут находиться рабочие места и места хранения ПДн при условии, что посетители и другие лица без полномочий не получают доступ к чужим документам, экранам и носителям. Руководитель подразделения определяет необходимые ограничения в рамках существующего режима помещения.

2.5. Конкретные цели обработки, категории субъектов, состав данных, сроки и правовые основания определяются Политикой, Положением, документированными процессами Университета и законодательством. Работнику запрещено расширять цель обработки по личному усмотрению или собирать сведения «на всякий случай».

2.6. Обработка специальных категорий персональных данных осуществляется при наличии правовых оснований, предусмотренных статьёй 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Обработка биометрических персональных данных осуществляется с соблюдением требований статьи 11 указанного Федерального закона, а также иных применимых нормативных правовых актов Российской Федерации.

3. ОТВЕТСТВЕННЫЕ ЛИЦА И РАЗДЕЛЕНИЕ ОБЯЗАННОСТЕЙ

3.1. Ректор обеспечивает утверждение локальных актов и назначение ответственных лиц. Университет как оператор несёт обязанности, установленные законодательством о ПДн. Распределение функций внутри организации не освобождает оператора от исполнения этих обязанностей.

3.2. Проректор по безопасности, назначенный приказом ректора ответственным за организацию обработки ПДн по статье 22.1 Закона № 152-ФЗ, обеспечивает общее руководство, координацию подразделений, организацию рассмотрения запросов субъектов и взаимодействия с Роскомнадзором, рассматривает представления о нарушениях и обеспечивает принятие организационных решений.

3.3. Начальник отдела безопасности организует предусмотренные приказом мероприятия по реагированию на инциденты и сбору материалов, обеспечивает взаимодействие с подразделениями и подготовку уведомлений. Обычное кадровое делопроизводство, хранение дел деканата и бухгалтерии не передаются ему только в силу занимаемой должности.

3.4. Главный специалист по защите информации отдела безопасности обеспечивает организационно-методическое сопровождение требований защиты, выполняет функции внутреннего контроля в объёме приказа ректора, проводит проверки, оформляет акты, ведёт контроль устранения нарушений и готовит предложения по улучшению мер. При проведении контроля он не подменяет непосредственных исполнителей и технических специалистов.

3.5. Начальник отдела информационной политики организует эксплуатацию и техническое сопровождение инфраструктуры Университета, включая реализацию порученных технических мер защиты и управление техническими правами доступа по утверждённым заявкам. Главный специалист по защите информации оценивает выполнение этих мер, но не обязан самостоятельно устанавливать и обслуживать каждое средство защиты.

3.6. Руководитель каждого структурного подразделения обеспечивает законную и безопасную обработку ПДн в своей деятельности: определяет работников, которым необходим доступ, места хранения документов, порядок обслуживания посетителей,

ознакомление сотрудников с правилами и устранение выявленных нарушений. Необходимые сведения допускается вести в уже действующих организационных документах.

3.7. Работники отдела кадров, деканатов, бухгалтерии, приёмной комиссии, архива и иные сотрудники, непосредственно обрабатывающие ПДн, являются уполномоченными исполнителями обработки, несущими ответственность за собственные действия и бездействие в пределах должностных функций, индивидуального допуска, полученных инструкций и закона.

3.8. При совмещении одной должностью нескольких функций принимаются меры по предотвращению конфликта интересов. Работник не должен единолично подтверждать надлежащее исполнение собственной деятельности как независимый проверяющий. При необходимости привлекается иное должностное лицо либо руководитель.

3.9. При необходимости руководитель подразделения определяет сотрудника, обеспечивающего хранение конкретных дел или выдачу ключей. Отдельный приказ или журнал для каждого шкафа не требуется, если обязанности и порядок доступа ясны из действующих документов и фактически соблюдаются.

4. ПОМЕЩЕНИЯ, МЕСТА ХРАНЕНИЯ И ОГРАНИЧЕНИЯ ДОСТУПА

4.1. Руководитель подразделения определяет перечень помещений, мест хранения бумажных ПДн и список работников, имеющих к ним доступ. Данные сведения фиксируются в локальных учетных формах подразделения (номенклатура дел, перечни допущенных лиц и т.п.) или в сводной форме (Приложение № 1). Оформление отдельных паспортов на кабинеты не требуется.

4.2. Места хранения бумажных ПДн должны позволять четко определить вид хранящихся документов, цели их обработки и круг допущенных лиц. Информация о задействованных информационных системах повторно не дублируется.

4.3. Руководитель подразделения обеспечивает актуализацию учетных сведений при существенном изменении мест хранения, состава документов или состава допущенных лиц. Плановое переоформление документов при неизменных условиях работы не требуется.

4.4. При неавтоматизированной обработке ПДн обеспечивается раздельное хранение документов, содержащих данные, которые обрабатываются в различных (несовместимых между собой) целях.

4.5. Если в кабинете ведется прием посетителей, зона их ожидания изолируется от рабочего пространства. Документы на столах и экраны компьютеров размещаются так, чтобы исключить визуальный доступ посторонних лиц к ПДн.

4.6. Серверное оборудование, средства резервного копирования и архивы с ПДн размещаются в специально оборудованных помещениях, исключающих доступ неуполномоченных лиц. Порядок доступа к ним регулируется регламентами профильных подразделений.

5. УСЛОВИЯ СЛУЖЕБНЫХ ПОМЕЩЕНИЙ И ФИЗИЧЕСКАЯ ЗАЩИТА

5.1. Рабочие места сотрудников (столы, мониторы, принтеры) организуются так, чтобы исключить визуальный доступ посторонних лиц к ПДн. При приеме посетителей или

краткосрочном покидании рабочего места сотрудники обязаны убирать документы из зоны видимости и блокировать экраны компьютеров.

5.2. Бумажные дела и съемные носители информации, содержащие ПДн, должны храниться в запираемых шкафах, сейфах, тумбах или картотеках. Конкретный способ хранения определяет руководитель подразделения исходя из объемов и характера обрабатываемых ПДн.

5.3. При отсутствии на рабочем месте уполномоченных сотрудников помещения и места хранения ПДн должны быть заперты. Запрещается оставлять ключи, электронные пропуска и пароли (коды доступа) в общедоступных местах или передавать их третьим лицам.

5.4. Порядок выдачи, возврата бумажных дел и доступа к ним в отсутствие основного работника определяется руководителем соответствующего подразделения. Дополнительный учет (например, ведение журналов выдачи ключей) вводится подразделением самостоятельно при фактической необходимости.

5.5. Проведение ремонтных, клининговых и технических работ сторонними лицами или техническими службами допускается только в присутствии сотрудника подразделения, либо после полного удаления (сокрытия) носителей ПДн из зоны проведения работ.

5.6. Запрещается оставлять документы и материальные носители, содержащие ПДн, на незащищенных поверхностях, в лотках принтеров/МФУ, в переговорных комнатах, коридорах и иных зонах общего пользования.

6. ПОРЯДОК ДОПУСКА РАБОТНИКОВ К ПДН И ПРЕКРАЩЕНИЯ ПОЛНОМОЧИЙ

6.1. Доступ работников к ПДн предоставляется исключительно при наличии служебной необходимости и в объеме, определяемом перечнем должностей, утверждаемым приказом ректора Университета.

6.2. Предоставление, изменение и блокировка прав доступа к ПДн осуществляются на основании обращений руководителей структурных подразделений через действующую в Университете систему электронного документооборота. Техническую реализацию прав доступа обеспечивает техническое подразделение.

6.3. До начала работы с ПДн работник обязан под подпись (в том числе электронную) ознакомиться с локальными нормативными актами Университета в сфере защиты ПДн, пройти инструктаж и принять на себя обязательства по соблюдению конфиденциальности.

6.4. Нахождение работника в помещении, где обрабатываются ПДн, не дает ему права доступа ко всем информационным системам и документам, расположенным в данном помещении. Права доступа строго разграничиваются по принципу минимальной достаточности для выполнения трудовых функций.

6.5. При увольнении работника, его переводе на другую должность или длительном изменении обязанностей руководитель подразделения обязан незамедлительно инициировать аннулирование (изменение) его прав доступа к информационным системам, а также организовать сдачу бумажных дел, материальных носителей и ключей.

6.6. Допуск к ПДн стажеров, практикантов или представителей подрядных организаций возможен только при наличии законных оснований, служебной необходимости и обязательного заключения соглашения (включения пункта) о конфиденциальности.

6.7. Работникам при работе с ПДн категорически запрещается:

• использовать чужие учетные записи, передавать свои пароли, токены или ключи доступа третьим лицам;

• предоставлять доступ к ПДн другим сотрудникам в обход установленного порядка;

• осуществлять самостоятельную выгрузку, копирование или передачу массивов ПДн, не связанных с выполнением текущего служебного задания.

7. ЕЖЕДНЕВНЫЕ ПРАВИЛА РАБОТЫ НА РАБОЧЕМ МЕСТЕ

7.1. Перед началом работы работник обязан авторизоваться под своей персональной учетной записью. При обнаружении признаков несанкционированного доступа к информационным системам или физическим местам хранения работник должен незамедлительно сообщить об этом в отдел безопасности.

7.2. В процессе работы допускается открывать и использовать только те документы (бумажные и электронные), которые необходимы для выполнения текущего служебного задания. При присутствии в кабинете посторонних лиц (посетителей) визуальный доступ к экрану компьютера и документам должен быть полностью перекрыт.

7.3. При любом, в том числе краткосрочном, покидании рабочего места работник обязан заблокировать компьютерный сеанс и убрать бумажные документы в запираемые места хранения. Наличие настроенной автоматической блокировки экрана не освобождает сотрудника от обязанности блокировать сеанс вручную.

7.4. При ведении телефонных разговоров, очных консультаций или видеоконференций передача ПДн допускается только после однозначной идентификации собеседника и проверки его полномочий. Запрещается озвучивать конфиденциальные сведения в присутствии посторонних лиц.

7.5. При отправке документов на печать работник обязан контролировать процесс вывода информации, своевременно и полностью забирать распечатки из лотка принтера/МФУ, а ошибочно напечатанные листы уничтожать способом, исключающим их восстановление.

7.6. По окончании рабочего дня работник обязан убрать все материальные носители ПДн в установленные места хранения, завершить рабочую сессию на компьютере, обесточить оргтехнику и запереть помещение в соответствии с действующим в Университете охранным режимом.

7.7. Работникам при работе с ПДн категорически запрещается:

• фотографировать или производить видеосъемку экранов мониторов и бумажных документов на личные мобильные устройства;

• отправлять рабочие документы и массивы ПДн на личную электронную почту или в личные мессенджеры;

• использовать несанкционированные публичные облачные хранилища;

• загружать ПДн во внешние публичные сервисы обработки текста и системы искусственного интеллекта (ИИ), если их использование прямо не разрешено локальными актами Университета.

8. РАБОТА С БУМАЖНЫМИ ДОКУМЕНТАМИ БЕЗ СРЕДСТВ АВТОМАТИЗАЦИИ

8.1. Сбор и использование бумажных документов, содержащих ПДн, осуществляются исключительно для достижения конкретных, заранее определенных целей. Документы, содержащие ПДн, обрабатываемые в разных (несовместимых) целях, должны храниться на отдельных материальных носителях и раздельно друг от друга.

8.2. При использовании типовых форм документов (анкеты, заявления, бланки) они должны содержать сведения о целях обработки, наименовании Оператора, правах субъекта, а также предусматривать отметку о согласии, если это требуется по закону.

8.3. Работникам запрещается изготавливать избыточные копии документов субъектов (паспортов, СНИЛС, дипломов, трудовых книжек, медицинских справок) при отсутствии прямой служебной необходимости и законных оснований для их архивного хранения.

8.4. Передача личных дел студентов и сотрудников и иных бумажных носителей содержащих ПДн между структурными подразделениями Университета должна фиксироваться способом, позволяющим установить получателя, дату передачи и факт возврата (через СЭД, внутренние реестры, описи или расписки). Создание дополнительных журналов учета не требуется, если фиксация уже ведется существующими методами.

8.5. Если на одном бумажном носителе содержатся ПДн, имеющие разные сроки хранения или подлежащие частичному уничтожению, работник обязан использовать методы, позволяющие уничтожить или заблокировать только требуемую часть данных (например, путем копирования лишь необходимых фрагментов или вымарывания).

8.6. При ведении бумажных журналов учета однократных посетителей на постах охраны сбор сведений ограничивается исключительно целями обеспечения безопасности. Использование данных из таких журналов в иных целях, а также их копирование неуполномоченными лицами категорически запрещено.

8.7. При обнаружении фактов утери бумажных документов (или отдельных листов из дел), их ошибочной подшивки, выдачи дел посторонним лицам или иных нарушений режима хранения, работник обязан незамедлительно прекратить работу и сообщить об инциденте в отдел безопасности (Раздел 15).

9. РАБОТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ И НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

9.1. Обработка ПДн в электронном виде допускается исключительно в санкционированных информационных системах Университета и только на учтенных служебных устройствах. Работники обязаны использовать только индивидуальные учетные записи и предоставленные им полномочия.

9.2. Работникам при работе в ИСПДн категорически запрещается:

• передавать пароли, токены и иные аутентификационные данные третьим лицам;

• самостоятельно отключать антивирусную защиту, средства журналирования (логирования) событий безопасности и иные элементы защиты информации;

• осуществлять несанкционированную установку стороннего программного обеспечения и подключать неучтенные внешние устройства (съемные носители).

9.3. Массовая выгрузка, экспорт или перенос ПДн из баз данных осуществляются строго в рамках должностных обязанностей и утвержденных бизнес-процессов Университета. Дополнительное согласование для штатных (предусмотренных функционалом системы) выгрузок не требуется.

9.4. Техническое подразделение обеспечивает технические меры защиты ИСПДн (идентификацию пользователей, управление доступом, регистрацию событий, антивирусную защиту и резервное копирование) в соответствии с требованиями Постановления Правительства РФ № 1119 и Приказа ФСТЭК России № 21. Конкретный комплекс мер фиксируется в технической документации на каждую систему.

9.5. В соответствии с ч. 5 ст. 18 ФЗ № 152-ФЗ, при сборе ПДн граждан Российской Федерации Университет обеспечивает запись, систематизацию, накопление, хранение, уточнение и извлечение данных с использованием баз данных, находящихся исключительно на территории РФ.

9.6. Использование съемных материальных носителей (флеш-накопителей, внешних жестких дисков) для переноса ПДн или отправки на печать допускается только на служебных устройствах вуза. Работники обязаны обеспечивать физическую сохранность таких носителей и исключать доступ к ним третьих лиц.

9.7. Дистанционная (удаленная) работа с ПДн допускается только с письменного разрешения Университета при условии организации защищенного канала доступа (VPN и др.). Работник обязан исключить возможность визуального доступа к ПДн со стороны членов семьи и иных посторонних лиц.

9.8. При обнаружении сбоев в работе ИСПДн, признаков вирусного заражения, получении подозрительных писем или фишинговых ссылок работник обязан незамедлительно сообщить об инциденте в отдел безопасности, не предпринимая самостоятельных действий по удалению программных логов или данных.

10. ПОЛУЧЕНИЕ ДАННЫХ И РАБОТА С СОГЛАСИЯМИ

10.1. До начала сбора новых ПДн структурное подразделение обязано определить конкретную законную цель, необходимый состав данных, правовое основание согласно ст. 6 ФЗ № 152-ФЗ и сроки их хранения. Избыточный сбор ПДн, не соответствующих целям обработки, категорически запрещен.

10.2. В случаях, когда обработка требует согласия субъекта, оно должно быть конкретным, предметным, информированным, сознательным и однозначным. В соответствии с ч. 1 ст. 9 ФЗ № 152-ФЗ, такое согласие оформляется в виде отдельного документа и не может быть объединено с иными договорами, заявлениями или анкетами.

10.3. Согласие на обработку ПДн, разрешенных субъектом для распространения (публикации на сайте Университета, в открытых списках и т.д.), оформляется исключительно

отдельно от основного согласия по правилам ст. 10.1 ФЗ № 152-ФЗ. Наличие общего согласия на обработку ПДн не дает права на публикацию этих данных.

10.4. При получении ПДн через представителя субъекта работник обязан проверить наличие и подлинность документов, подтверждающих его полномочия (доверенность, свидетельство о рождении для несовершеннолетних, документы об опеке).

10.5. Сбор и обработка специальных категорий ПДн (включая сведения о состоянии здоровья, инвалидности, ограничениях возможностей здоровья) допускаются только при наличии прямых законных оснований. Доступ к медицинским документам строго ограничивается минимальным кругом уполномоченных лиц.

10.6. Университет обеспечивает централизованное хранение и учет всех полученных согласий и документов, подтверждающих правовые основания обработки, для подтверждения законности процедур. Подписание работником ознакомительного листа с настоящим Регламентом не заменяет получение его согласия на обработку ПДн.

11. ПЕРЕДАЧА ПДН, ПЕРЕПИСКА, ПОСЕТИТЕЛИ И ТРЕТЬИ ЛИЦА

11.1. При внутренней передаче ПДн работник обязан предварительно проверить полномочия получателя и ограничить объем сведений служебной необходимостью. Наличие у коллеги корпоративной электронной почты само по себе не является основанием для предоставления ему доступа к ПДн.

11.2. Перед отправкой электронных писем работник обязан проверять корректность адреса получателя и состав вложений. Массовые рассылки внешним адресатам должны осуществляться способом, исключающим раскрытие адресов и данных других получателей (например, через скрытую копию).

11.3. Категорически запрещается передача ПДн через личные почтовые сервисы, неслужебные мессенджеры и публичные файлообменники. Использование внешних каналов связи допускается только при условии применения утвержденных в Университете средств защиты информации.

11.4. Передача ПДн внешним лицам и организациям (включая родственников субъектов, сторонние образовательные организации, работодателей) допускается только при наличии законных оснований и согласия субъекта. При передаче ПДн работников обязательно соблюдение требований ст. 88 Трудового кодекса РФ.

11.5. Предоставление ПДн государственным органам осуществляется только на основании мотивированных официальных запросов в пределах их компетенции. При возникновении сомнений в законности запроса работник обязан передать его руководителю подразделения для правовой оценки.

11.6. Поручение обработки ПДн внешним подрядчикам допускается строго при наличии правовых оснований и оформления договора в соответствии с ч. 3 ст. 6 ФЗ № 152-ФЗ. Заключение хозяйственных договоров (поставка, клининг и др.) не дает подрядчикам права доступа к ПДн.

11.7. Публикация на официальных ресурсах Университета списков поступающих, обучающихся или сотрудников, а также результатов экзаменов осуществляется строго в объеме, предусмотренном законодательством. При наличии технической возможности приоритет отдается использованию обезличенных идентификаторов (номеров СНИЛС, ID-кодов).

12. ОСОБЕННОСТИ РАБОТЫ ОТДЕЛЬНЫХ ПОДРАЗДЕЛЕНИЙ

12.1. Отдел кадров: обеспечивает хранение личных дел, трудовых книжек и договоров в запираемых шкафах (сейфах) с разграничением доступа сотрудников по должностным функциям. Прием работников и кандидатов осуществляется способом, исключающим визуальный доступ посторонних лиц к чужим документам.

12.2. Деканаты факультетов и учебные подразделения: используют личные дела обучающихся, зачетные книжки, ведомости и сведения о законных представителях исключительно для обеспечения учебного процесса. Категорически запрещается публикация списков студентов с указанием их ПДн (телефоны, адреса, даты рождения) в публичных группах и чатах мессенджеров.

12.3. Приемная комиссия: осуществляет прием документов поступающих строго через официальные каналы (СЭД, суперсервис «Поступление в вуз онлайн», личный кабинет). Публикация конкурсных списков и результатов экзаменов организуется с соблюдением специальных норм приема и минимизацией раскрываемых ПДн.

12.4. Управление бухгалтерского учета и финансового контроля: обрабатывает сведения о доходах, банковских реквизитах и договорах исключительно для проведения расчетов, налогового учета и сдачи отчетности. Доступ к бухгалтерским базам данных строго разграничивается.

12.5. Отдел безопасности и бюро пропусков: осуществляют сбор данных посетителей для ведения журналов СКУД исключительно в целях обеспечения пропускного режима. Просмотр и выгрузка записей камер видеонаблюдения допускаются только уполномоченными лицами при расследовании инцидентов.

12.6. Архив: организует прием, учет и хранение личных дел архивного фонда в соответствии с утвержденной номенклатурой дел. Уничтожение документов с истекшими сроками хранения производится только после проведения экспертизы ценности в соответствии с архивным законодательством РФ.

12.7. Руководители структурных подразделений вправе издавать внутренние рабочие инструкции, детализирующие порядок обработки ПДн на конкретных рабочих местах, при условии их полного соответствия настоящему Регламенту.

13. ХРАНЕНИЕ, АРХИВИРОВАНИЕ, УНИЧТОЖЕНИЕ

13.1. Персональные данные хранятся не дольше, чем этого требуют цели их обработки, за исключением случаев, когда срок хранения установлен федеральным законом, договором или правилами архивного дела. Сроки хранения документов конкретизируются в утвержденной Номенклатуре дел Университета.

13.2. Уничтожение документов и материальных носителей, содержащих ПДн, производится при наступлении следующих оснований: достижение целей обработки, отзыв согласия субъектом, выявление неправомерной обработки (если устранить нарушение невозможно) или истечение установленных сроков хранения. Категорически запрещается утилизация бумажных документов и цифровых носителей с ПДн через общие контейнеры для мусора.

13.3. Бумажные носители уничтожаются способом, полностью исключающим возможность восстановления текста (путем шредирования или термического уничтожения). Уничтожение электронных данных из ИСПДн и резервных копий обеспечивается техническим подразделением путем гарантированного стирания без возможности программного восстановления.

13.4. В соответствии с Приказом Роскомнадзора от 28.10.2022 № 179, факт уничтожения ПДн подтверждается следующими обязательными документами:

• при неавтоматизированной обработке — Актом об уничтожении персональных данных;

• при обработке в ИСПДн — Актом об уничтожении персональных данных и Выгрузкой из журнала регистрации событий (логов) информационной системы.

13.5. Если штатный функционал ИСПДн не позволяет внести в выгрузку логов все требуемые Приказом № 179 сведения, недостающие данные вносятся непосредственно в текст Акта об уничтожении. Акты и выгрузки журналов подлежат хранению в Университете в течение 3 лет с момента уничтожения данных.

13.6. Процедуру уничтожения организует подразделение, ответственное за хранение соответствующих документов или ресурса. Главный специалист по защите информации отдела безопасности вправе осуществлять выборочную проверку соблюдения установленного порядка в рамках планового или внепланового внутреннего контроля.

14. ЗАПРОСЫ И ОБРАЩЕНИЯ СУБЪЕКТОВ ПДН

14.1. При получении запроса от субъекта ПДн, его представителя или Роскомнадзора работник обязан незамедлительно зарегистрировать его в системе электронного документооборота Университета для передачи ответственному лицу. Предоставление устных ответов или самостоятельная отправка электронных писем с раскрытием ПДн работниками категорически запрещены.

14.2. При рассмотрении поступившего обращения в обязательном порядке проверяются личность заявителя (или полномочия его представителя), суть требований и наличие законных оснований для обработки. При подтверждении фактов неточности данных или неправомерности их обработки Университет осуществляет уточнение, блокирование или уничтожение ПДн в установленные законом сроки.

14.3. Проректор по безопасности, как лицо, ответственное за организацию обработки ПДн в Университете, координирует рассмотрение обращений и контролирует соблюдение сроков ответа. Структурные подразделения обязаны оперативно предоставлять фактические сведения по запросу отдела безопасности для подготовки мотивированного ответа.

15. НАРУШЕНИЯ РЕЖИМА И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ

15.1. Признаками возможного нарушения являются, в частности: потеря личного дела; письмо не тому адресату; обнаружение ПДн в публичном доступе; просмотр записи СКУД без полномочий; несанкционированный вход в учётную запись; заражение устройства; обнаружение незапертого места хранения при отсутствии ответственных.

16. ВНУТРЕННИЙ КОНТРОЛЬ, ФИКСАЦИЯ МЕР И ПРОВЕРКА КАБИНЕТОВ

16.1. Руководитель структурного подразделения осуществляет текущий контроль соблюдения режима безопасности ПДн на рабочих местах подчинённых работников и незамедлительно устраняет выявленные нарушения. Для проведения самопроверок руководителем может использоваться контрольный лист (Приложение № 3). Обязательное ежедневное заполнение контрольного листа при открытии и закрытии каждого кабинета не предусматривается.

16.2. Главный специалист по защите информации осуществляет выборочный внутренний контроль соблюдения требований защиты персональных данных в соответствии с утверждённым планом, а также участвует во внеплановых проверках по поручению уполномоченного руководства Университета в пределах своей компетенции.

По результатам проверок при выявлении нарушений оформляются акты или служебные записки с указанием выявленных замечаний. Организацию устранения нарушений обеспечивают руководители соответствующих структурных подразделений.

16.3. Руководители подразделений обязаны обеспечивать проверяющему лицу беспрепятственный доступ в помещения и к запрашиваемым учетным документам в рамках его полномочий. Проверки проводятся с обязательным соблюдением конфиденциальности ПДн и минимизацией копирования проверяемых материалов.

16.4. Учёт и хранение материалов проверок организуются отделом безопасности с использованием действующей системы документооборота Университета в соответствии с утверждённой номенклатурой дел.

17. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ И РУКОВОДИТЕЛЕЙ

17.1. Назначение должностных лиц, ответственных за организацию обработки и обеспечение безопасности ПДн, не снимает с Университета общих обязательств Оператора, установленных законодательством РФ.

17.2. Персональная ответственность в Университете распределяется следующим образом:

• Руководитель структурного подразделения несет ответственность за организацию процессов обработки ПДн в своем отделе, контроль допусков подчиненных, обеспечение условий безопасного хранения носителей, своевременный инструктаж работников и исполнение предписаний отдела безопасности.

• Непосредственный исполнитель (работник) несет персональную ответственность за сохранность вверенных ему документов, соблюдение ИБ-режима на рабочем месте и законность совершаемых им операций с ПДн.

17.3. Руководство Университета (проректор по безопасности, начальник отдела безопасности, руководитель технического подразделения и главный специалист по защите информации) несут ответственность строго в пределах закрепленных за ними трудовыми договорами, должностными инструкциями и приказами ректора полномочий.

17.4. За нарушение требований настоящего Регламента, повлекшее неправомерный доступ, блокирование, изменение, копирование или распространение ПДн, работники Университета привлекаются к дисциплинарной ответственности в порядке, предусмотренном ст. 192–193 Трудового кодекса РФ.

17.5. В случае причинения Университету прямого действительного ущерба вследствие неправомерных действий с ПДн (включая необходимость выплаты штрафов контролирующих органов по вине работника), виновное лицо привлекается к материальной ответственности в соответствии со ст. 238–243 Трудового кодекса РФ.

17.6. В случаях, предусмотренных законодательством Российской Федерации, виновные лица могут быть привлечены к административной (по ст. 13.11 КоАП РФ), гражданско-правовой или уголовной ответственности (включая ст. 137, 272 УК РФ).

17.7. Грубыми нарушениями настоящего Регламента, влекущими за собой инициирование служебного расследования, являются:

• несанкционированная передача личных дел или массивов ПДн третьим лицам;

• выгрузка (копирование) баз данных Университета в личных, коммерческих или иных целях, не связанных со служебным заданием;

• компрометация, передача или использование чужих паролей и токенов доступа;

• умышленное сокрытие факта инцидента безопасности ПДн;

• ненадлежащее утилизирование бумажных или электронных носителей (в обход требований раздела 13).

18. ПОРЯДОК ВНЕДРЕНИЯ И ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

18.1. Настоящий Регламент вступает в силу после его утверждения ректором Университета и ознакомления работников в установленном порядке. Исполнение требований Регламента организуется преимущественно в рамках действующего документооборота, без создания избыточных журналов и ежедневной отчетности.

18.2. Руководители структурных подразделений определяют места хранения бумажных ПДн и круг допущенных лиц, а также обеспечивают соблюдение ИБ-режима в кабинетах. Для фиксации этих сведений используется рекомендованная сводная форма (Приложение № 1) либо соответствующие изменения вносятся в существующие документы подразделения. Оформление отдельных паспортов на каждый кабинет не требуется.

18.3. В помещениях со смешанным режимом (одновременный прием посетителей и хранение документов) руководитель подразделения определяет организационные и

технические меры защиты, не препятствующие исполнению текущих функций отдела, и при необходимости согласовывает их с проректором по безопасности.

18.4. Главный специалист по защите информации отдела безопасности оказывает структурным подразделениям методическое сопровождение и проверяет соблюдение требований в рамках внутреннего контроля, не подменяя при этом руководителей подразделений и непосредственных исполнителей.

18.5. Пересмотр и актуализация Регламента проводятся при существенном изменении законодательства РФ, модернизации процессов обработки ПДн в Университете или при выявлении недостаточности установленных мер защиты. Изменения утверждаются в установленном в Университете порядке.

Приложение № 1
к Регламенту организации работы
с персональными данными

СВЕДЕНИЯ О МЕСТАХ ОБРАБОТКИ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ (РЕКОМЕНДУЕМАЯ ФОРМА)

Заполняется при необходимости по подразделению. Если соответствующие сведения уже имеются в номенклатуре дел, перечне допущенных работников или иной документации, отдельная форма не ведётся.

Реквизит	**Сведения (при необходимости)**
Подразделение / руководитель	_____
Места хранения бумажных ПДн (корпус, кабинет, шкаф, архив)	_____
Категории документов и цели обработки	_____
Работники, имеющие доступ (должности / ссылка на перечень)	_____
Как ограничивается доступ посторонних	_____
Используемые действующие учётные документы	_____
Кто отвечает за актуальность сведений	_____
Дата проверки / актуализации	_____

Примечание: форма предназначена для практического учёта мест хранения и доступа, а не для установления специальных категорий помещений.

Приложение № 2
к Регламенту организации работы
с персональными данными

ПАМЯТКА СОТРУДНИКУ

ПРАВИЛА ПЕРЕД НАЧАЛОМ, ВО ВРЕМЯ И ПОСЛЕ РАБОТЫ

☐ Перед началом смены: убедиться, что ключи и документы находятся в установленном месте; войти только под своей учётной записью; проверить отсутствие несанкционированного доступа и открытых чужих документов.

☐ При работе с посетителем: убрать чужие документы и носители, закрыть не относящиеся к обращению вкладки и файлы, исключить просмотр экранов и иных сведений посторонними.

☐ При временном уходе: заблокировать компьютер, убрать дела и распечатки, не оставлять служебные средства доступа без присмотра.

☐ Перед отправкой информации: сверить адресата, полномочия, вложения, объём и защищённость канала; не использовать личные почтовые ящики и неразрешённые облачные сервисы.

☐ При работе с личным делом: получить и передать его по установленному маршруту; не делать лишних копий; не складывать документы в общедоступные лотки и открытые шкафы.

☐ При обнаружении инцидента: незамедлительно известить руководителя и главного специалиста по защите информации отдела безопасности; не удалять следы; выполнять отдельный Регламент реагирования.

☐ Перед уходом: убрать документы, проверить принтер/сканер, закрыть доступные места хранения, заблокировать или завершить сессию, вернуть ключи и закрыть помещение по установленному порядку.

Примечание: эта памятка не заменяет ознакомление с полным Регламентом.

Приложение № 3 к Регламенту организации работы с персональными данными

КОНТРОЛЬНЫЙ ЛИСТ

ВЫБОРОЧНОЙ ПРОВЕРКИ ОБРАБОТКИ ПДн

№	Проверяемое требование	Да / нет / н/п	Замечание / срок
1	Определены места хранения бумажных ПДн и допущенные работники		
2	Посетители не имеют доступа к чужим документам и экранам		
3	Категории обрабатываемых ПДн и цели понятны сотрудникам		
4	Перечень допущенных лиц соответствует выполняемым функциям		
5	Новые сотрудники ознакомлены под подпись с применимыми правилами		
6	Документы хранятся в закрываемых местах с ограниченным доступом		
7	Бумажные носители разных несовместимых целей хранятся раздельно		
8	Ключи и средства доступа не оставлены в общедоступных местах		
9	Принтеры / сканеры / лотки печати не содержат открытых ПДн		
10	Рабочие компьютеры блокируются при отсутствии сотрудников		
11	Нет общих учётных записей и передачи паролей между сотрудниками		
12	Права доступа изменяются после кадровых изменений		
13	Выгрузки ПДн и съёмные носители учтены по установленному порядку		
14	Отправки по почте и передачи данных происходят только по правовому основанию		
15	Лишние копии и рабочие файлы своевременно удаляются / уничтожаются		
16	При обнаружении нарушений соблюдён маршрут оповещения		
17	Ранее выявленные нарушения устранены и документально подтверждены		

Кабинет № _____ Подразделение _____ Дата _____

Проверяющий _____ Руководитель подразделения _____

МАТРИЦА РАСПРЕДЕЛЕНИЯ ОРГАНИЗАЦИОННЫХ И ИСПОЛНИТЕЛЬСКИХ ФУНКЦИЙ

Задача	**Организация / исполнение**	**Контроль / согласование**
Правовые основания и общая организация обработки	Проректор по безопасности, руководители процессов	Ректор; уполномоченный внутренний контроль
Допуск сотрудников / актуальность прав	Руководитель подразделения; техническое подразделение — техническое оформление	Главный специалист по защите информации — проверка
Места хранения, ключи, доступ	Руководитель подразделения и назначенные исполнители	Главный специалист по защите информации — проверка
Работа с бумажными и электронными делами	Уполномоченный работник	Руководитель подразделения; внутренний контроль
Техническая настройка ИС и СЗИ	Отдел информационной политики	Главный специалист по защите информации — профильный контроль
Разбор инцидента и сбор доказательств	Начальник отдела безопасности; технические и профильные подразделения	Проректор по безопасности; главный специалист — контроль
Уведомления об утечках	Уполномоченный отправитель; начальник отдела безопасности, главный специалист — организация;	Проректор по безопасности — организация и согласование
Уничтожение и архивирование дел	Руководители профильных подразделений, делопроизводство, ИТ	Главный специалист — проверка в своей компетенции

Примечание: данная матрица разъясняет функции в пределах действующих приказов; при расхождении с действующим распорядительным актом приоритет имеет действующий акт в рамках законодательства.

ПРАВОВЫЕ ОСНОВАНИЯ И ГРАНИЦЫ ПРИМЕНЕНИЯ ТРЕБОВАНИЙ

НПА	**Что регулирует / где используется**
152-ФЗ, ст. 3, 5, 6, 7, 9–11, 18, 18.1, 19, 21, 22.1	Статус оператора, основания обработки, конфиденциальность, согласия, права субъектов, защита, обязанности ответственного, сроки при инцидентах
Постановление Правительства РФ № 687, п. 4–15	Бумажные носители, уведомление сотрудников о правилах обработки, раздельное хранение и доступ, формы документов и журналов
Постановление Правительства РФ № 1119	Требования и уровни защищённости ПДн в информационных системах
Приказ ФСТЭК России № 21	Конкретизация применимых технических и организационных мер для ИСПДн
Приказ Роскомнадзора № 179	Подтверждение уничтожения ПДн актами и, при автоматизации, выгрузкой из журнала ИСПДн
ТК РФ, ст. 86–90; 192–193; 238–243	Обработка и передача ПДн работника, дисциплинарная и материальная ответственность
КоАП РФ, ст. 13.11; УК РФ — применимые составы	Административная и уголовная ответственность при наличии признаков состава правонарушения
Локальные акты АГПУ	Фактическое распределение ролей, сроки внутреннего оповещения, маршрут передачи дел, режим ключей, проверка кабинетов

Примечание: законодательство не требует для любого кабинета обязательного отдельного паспорта, одинакового сейфа, журнала ключей, ежедневного заполнения чек-листа или выделения помещений в буквенные зоны. При этом обязанности обеспечивать законную обработку ПДн, определять места хранения и лиц с доступом, сохранять конфиденциальность и подтверждать уничтожение ПДн в предусмотренных случаях сохраняются.

При изменении законодательства, порядка обработки ПДн или штатной структуры Регламент пересматривается по мере необходимости в установленном Университетом порядке.

Ректору
ФГБОУ ВО «Армавирского государственного педагогического университета»
Нижнику Е.А.
352901, Краснодарский край, г. Армавир,
ул. Розы Люксембург, д. 159

СВЕДЕНИЯ О СУБЪЕКТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	
Фамилия, имя, отчество	
Дата рождения	
Паспорт	серия _____ номер _____
Кем и когда выдан	
Адрес регистрации	
Телефон	
Адрес электронной почты	
Отношение к АГПУ	☐ обучающийся ☐ выпускник ☐ работник ☐ абитуриент ☐ иное: _____
Факультет / подразделение, группа (при наличии)	

ОТЗЫВ СОГЛАСИЯ
на обработку персональных данных

В соответствии с частью 2 статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» отзываю согласие на обработку моих персональных данных, ранее данное ФГБОУ ВО «Армавирскому государственному педагогическому университету» (далее — ФГБОУ ВО «АГПУ»):

☐ полностью;

☐ в части следующих целей / данных: _____

_____

(например: размещение фотографии на сайте и в социальных сетях Университета)

Прошу прекратить обработку указанных персональных данных и уничтожить их в срок, не превышающий 30 дней с даты поступления настоящего отзыва (ч. 5 ст. 21 Федерального закона № 152-ФЗ).

Мне известно, что ФГБОУ ВО «АГПУ» вправе продолжить обработку персональных данных без моего согласия в случаях, предусмотренных законодательством Российской Федерации (в том числе хранение личного дела, документов об образовании и архивных документов в установленные сроки).

Ответ о результатах рассмотрения прошу:

☐ направить на e-mail ☐ направить почтой ☐ выдать лично

«____» _____ 20___ г. _____ _____

(подпись) *(фамилия, инициалы)*

ОТМЕТКА О ПРИНЯТИИ (заполняется сотрудником Университета)

Вх. № _____ от «____» _____ 20___ г.

Принял: _____ _____ _____

(должность) *(подпись)* *(фамилия, инициалы)*