Федеральное государственное бюджетное образовательное учреждение дополнительного профессионального образования «Санкт-Петербургский институт управления и пищевых технологий» (ФГБОУ ДПО СПИУПТ)

УТВЕРЖДАЮ:
Врио ректора
_____ И.Н. Прохорчик
«12» ноября 2026 г.
М.П.

ПРИНЯТО
на заседании Ученого совета
«12» ноября 2026 г.
Протокол № 10

ПОЛИТИКА

защиты и обработки персональных данных

федерального государственного бюджетного образовательного учреждения дополнительного профессионального образования «Санкт-Петербургский институт управления и пищевых технологий»

(ФГБОУ ДПО СПИУПТ)

1. Общие положения

1.1. Настоящая Политика в отношении обработки персональных данных (далее — Политика) разработана во исполнение требований ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 26.07.2026) «О персональных данных» (далее — Закон о персональных данных) в целях 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.

1.2. Политика действует в отношении всех персональных данных, которые обрабатывает федеральное государственное бюджетное образовательное учреждение дополнительного профессионального образования «Санкт-Петербургский институт управления и пищевых технологий» (далее — Оператор, ФГБОУ ДПО СПИУПТ).

1.3. Политика распространяется на отношения в области обработки персональных данных, возникшие у Оператора как до, так и после утверждения настоящей Политики.

1.4. Во исполнение требований ч. 2 ст. 18.1 Закона о персональных данных Политика публикуется в свободном доступе в информационно-телекоммуникационной сети «Интернет» на сайте Оператора.

1.5. Политика разработана с учётом Трудового кодекса РФ, Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 04.08.2026) «Об образовании в Российской Федерации», постановления Правительства РФ от 27.11.2025 № 1912 «Об утверждении Правил предоставления

гостиничных услуг и услуг иных средств размещения в Российской Федерации», приказа Роскомнадзора от 28.10.2022 № 179 и Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения (утв. приказом Росархива от 20.12.2019 № 236; далее — Перечень № 236).

2. Термины и принятые сокращения

Персональные данные (ПД) — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешённые субъектом персональных данных для распространения, — персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путём дачи согласия на их обработку и распространение (ст. 10.1 Закона о персональных данных).

Оператор персональных данных (Оператор) — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных — любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемые с использованием средств автоматизации или без их использования, в том числе: сбор; запись; систематизация; накопление; хранение; уточнение (обновление, изменение); извлечение; использование; передача (предоставление, доступ); распространение; обезличивание; блокирование; удаление; уничтожение.

Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

Предоставление персональных данных — действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных (с 01.09.2025 обезличивание осуществляется в порядке, установленном приказом Роскомнадзора от 19.06.2025 № 140).

Информационная система персональных данных (ИСПД) — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Защита персональных данных — деятельность, направленная на предотвращение утечки защищаемых персональных данных, несанкционированных и непреднамеренных воздействий на защищаемые персональные данные.

3. Правовые основания, цели и условия обработки персональных данных

3.1. Общие условия обработки

3.1.1. Обработка персональных данных осуществляется Оператором в соответствии с требованиями законодательства Российской Федерации.

3.1.2. Обработка осуществляется как с использованием средств автоматизации, так и без их использования.

3.1.3. К обработке персональных данных допускаются работники Оператора, в должностные обязанности которых входит обработка персональных данных.

3.1.4. Обработка осуществляется путём получения персональных данных в устной и письменной форме, внесения их в журналы, реестры и информационные системы Оператора, а также иными способами, предусмотренными локальными нормативными актами.

3.1.5. Не допускается раскрытие третьим лицам и распространение персональных данных без согласия субъекта, если иное не предусмотрено федеральным законом. Передача персональных данных органам дознания и следствия, ФНС России, Социальному фонду России и иным уполномоченным органам осуществляется в соответствии с законодательством Российской Федерации (ст. 88 ТК РФ).

3.1.6. При сборе персональных данных, в том числе посредством 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 (ч. 5 ст. 18 Закона о персональных данных).

3.2. Правовые основания обработки

3.2.1. Обработка персональных данных осуществляется только при наличии правовых оснований, предусмотренных ч. 1 ст. 6 Закона о персональных данных, в частности:

— субъект персональных данных дал согласие на обработку (ст. 9 Закона о персональных данных);

— обработка необходима для достижения целей, предусмотренных федеральными законами, для осуществления и выполнения возложенных законодательством на Оператора функций, полномочий и обязанностей (трудовое законодательство, законодательство о налогах и сборах, о бухгалтерском учёте, об образовании, о социальном и пенсионном страховании, о воинском учёте, о противодействии терроризму);

— обработка необходима для исполнения договора, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных (трудовой договор, гражданско-правовой договор, договор об образовании, договор найма жилого помещения в общежитии, договор об оказании гостиничных услуг);

— для осуществления прав и законных интересов Оператора или третьих лиц, если при этом не нарушаются права и свободы субъекта персональных данных;

— в связи с участием в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах, а также для исполнения судебного акта, акта другого органа или должностного лица в соответствии с законодательством Российской Федерации об исполнительном производстве;

— для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно.

3.3. Согласие на обработку персональных данных

3.3.1. Согласие субъекта запрашивается только тогда, когда обработка не может быть законно обоснована иным основанием, предусмотренным ч. 1 ст. 6 Закона о персональных данных; применительно к работникам — с учётом ст. 86 Трудового кодекса РФ.

3.3.2. Согласие оформляется отдельно по каждой цели обработки, содержит сведения, предусмотренные ч. 4 ст. 9 Закона о персональных данных, и может быть отозвано субъектом в любой момент.

3.3.3. Отдельное письменное согласие оформляется на обработку специальных категорий персональных данных (ст. 10), биометрических персональных данных (ст. 11) и персональных данных, разрешённых для распространения (ст. 10.1).

3.3.4. Согласие на обработку персональных данных, разрешённых субъектом для распространения, может быть предоставлено Оператору непосредственно либо с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

3.4. Принципы обработки

3.4.1. Обрабатываются только персональные данные, отвечающие целям обработки; обрабатываемые данные не должны быть избыточными по отношению к заявленным целям (ч. 5 ст. 5 Закона о персональных данных).

3.4.2. По каждой цели обработки в локальных нормативных актах Оператора определены категории субъектов, перечни обрабатываемых персональных данных, способы обработки, сроки обработки и хранения (ч. 2 ст. 18.1 Закона о персональных данных).

3.5. Цели обработки персональных данных

Цель 1. Ведение кадрового учёта и обеспечение трудовых отношений с работниками.

Правовые основания: ст. 86 ТК РФ; п. 2 и 3 ч. 1 ст. 6 Закона о персональных данных; Федеральный закон от 28.03.1998 № 53-ФЗ (ред. от 04.08.2026) «О воинской обязанности и военной службе» и постановление Правительства РФ от 27.11.2006 (ред. от 24.03.2026) № 719; законодательство о социальном страховании.

Субъекты: работники Оператора, в том числе бывшие работники.

Перечень персональных данных (общие): фамилия, имя, отчество; дата рождения; пол; гражданство; адреса регистрации и места жительства; данные документа, удостоверяющего личность; СНИЛС; ИНН; сведения об образовании; сведения о профессии и занимаемой должности; сведения о трудовой деятельности и стаже; отношение к воинской обязанности и сведения о воинском учёте; семейное положение и сведения о детях (в целях предоставления социальных гарантий и стандартных налоговых вычетов); номер расчётного счёта; контактный телефон; адрес электронной почты; данные водительского удостоверения (только для водителей и работников, использующих личный транспорт в служебных целях).

Специальные категории: сведения о состоянии здоровья — исключительно в объёме, необходимом для охраны труда и проведения обязательных медицинских осмотров (ст. 214, 220 ТК РФ), предоставления гарантий по состоянию здоровья (ст. 254 ТК РФ) и учёта сведений о временной нетрудоспособности, передаваемых из Социального фонда России.

Сроки: в период действия трудового договора; после прекращения — сроки хранения кадровых документов по Перечню № 236. Срок хранения в информационных системах соответствует сроку хранения аналогичных бумажных документов.

Цель 2. Заключение и исполнение гражданско-правовых договоров с физическими лицами (преподаватели, привлекаемые к образовательной деятельности, авторы, подрядчики, исполнители услуг).

Правовые основания: п. 5 ч. 1 ст. 6 Закона о персональных данных; Гражданский кодекс РФ; Налоговый кодекс РФ (гл. 23 «Налог на доходы физических лиц», гл. 34 «Страховые взносы»); Федеральный закон от 06.12.2011 № 402-ФЗ (ред. от 15.12.2025) «О бухгалтерском учёте» (в части первичных учётных документов).

Субъекты: физические лица, состоящие с Оператором в гражданско-правовых отношениях.

Перечень персональных данных: фамилия, имя, отчество; дата рождения; гражданство; данные документа, удостоверяющего личность; ИНН; СНИЛС; адрес регистрации и места жительства; номер расчётного счёта; контактный телефон; адрес электронной почты; сведения об

образовании и квалификации (для договоров об оказании образовательных услуг и услуг по созданию контента); сведения о доходах по договору.

Сроки: в период действия договора и не менее 5 лет после его завершения (первичные учётные документы — НК РФ, ст. 29 Федерального закона № 402-ФЗ); договоры, акты и иные документы — в сроки, установленные Перечнем № 236.

Цель 3. Ведение бухгалтерского учёта, исполнение требований законодательства о налогах и сборах и о страховых взносах.

Правовые основания: п. 2 ч. 1 ст. 6 Закона о персональных данных; Налоговый кодекс РФ (ред. от 04.08.2026); Федеральный закон от 06.12.2011 № 402-ФЗ (ред. от 15.12.2025) «О бухгалтерском учёте».

Субъекты: работники Оператора.

Перечень персональных данных: фамилия, имя, отчество; дата рождения; данные документа, удостоверяющего личность; СНИЛС; ИНН; сведения о доходах и удержанных суммах; сведения о детях и иных лицах, находящихся на иждивении (в целях стандартных налоговых вычетов); номер расчётного счёта; номер лицевого счёта.

Сроки: не менее 5 лет (НК РФ, ст. 29 Федерального закона № 402-ФЗ); расчётно-платёжные ведомости — 6 лет в случаях, предусмотренных Перечнем № 236.

Цель 4. Представление отчётности и сведений в уполномоченные органы.

Правовые основания: п. 2 ч. 1 ст. 6 Закона о персональных данных. Передача персональных данных в ФНС России, Социальный фонд России, Роскомнадзор, военные комиссариаты, органы внутренних дел и дознания осуществляется только в объёме, предусмотренном соответствующим федеральным законом или запросом.

Цель 5. Подбор персонала, рассмотрение кандидатов на вакантные должности.

Правовые основания: п. 4 ч. 1 ст. 6 Закона о персональных данных (права и законные интересы Оператора); при включении кандидата в кадровый резерв — согласие кандидата.

Субъекты: кандидаты на трудоустройство.

Перечень персональных данных: фамилия, имя, отчество; дата рождения; гражданство; адрес регистрации; номер телефона; адрес электронной почты; сведения об образовании; сведения о профессии и занимаемой должности; сведения о трудовом стаже и квалификации; сведения, содержащиеся в резюме кандидата.

Сроки: до принятия решения о приёме на работу; при отсутствии решения — в течение одного года с даты получения персональных данных; с согласия кандидата — на срок действия согласия (включение в кадровый резерв). По истечении срока персональные данные уничтожаются в течение 30 дней.

Цель 6. Заключение и исполнение договоров на оказание образовательных услуг по дополнительным профессиональным программам повышения квалификации и профессиональной переподготовки, оформление и выдача документов о квалификации, а также внесение сведений о полученных документах об образовании и (или) о квалификации, документах об обучении в федеральную информационную систему «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (ФИС ФРДО).

Правовые основания: п. 3 ч. 1 ст. 6 Закона о персональных данных (договор об образовании); ст. 53, 76, 97 Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 04.08.2026) «Об образовании в Российской Федерации».

Субъекты: слушатели дополнительных профессиональных программ.

Перечень персональных данных: фамилия, имя, отчество; дата рождения; гражданство; данные документа, удостоверяющего личность; СНИЛС; сведения о документе об образовании; сведения о должности и месте работы (при направлении работодателем); контактный телефон; адрес электронной почты.

Сроки: период обучения и 5 лет после его завершения (договоры об образовании, акты); документы, подтверждающие освоение программ, — в сроки, установленные Перечнем № 236.

Цель 7. Размещение на официальном сайте сведений о руководителе, его заместителях, педагогических и иных работниках в целях информационной открытости ФГБОУ ДПО СПИУПТ.

Правовые основания: пп. 1, 2 ч. 1 ст. 6 Закона о персональных данных (согласие субъекта; исполнение обязанности, возложенной законом); ст. 10.1 Закона о персональных данных (согласие на распространение ПД неопределённому кругу лиц); п. 5 ч. 1 ст. 6 Закона о персональных данных (трудовой договор — для работников по основному месту работы, в том числе по внутреннему совместительству; гражданско-правовой договор — при условии включения в него обязательства о размещении сведений на официальном сайте); п. 6 ч. 2 ст. 29, ч. 1 ст. 97 Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 04.08.2026) «Об образовании в Российской Федерации»; ст. 86, 89 ТК РФ.

Субъекты: руководитель ФГБОУ ДПО СПИУПТ, его заместители; педагогические работники, состоящие с Оператором в трудовых отношениях по основному месту работы, в том числе по внутреннему совместительству; педагогические работники по внешнему совместительству; физические лица, привлекаемые к образовательной деятельности по гражданско-правовым договорам.

Перечень персональных данных:

общий: фамилия, имя, отчество; фотография; занимаемая должность; сведения об уровне образования и квалификации; сведения об учёной степени и учёном звании (при наличии); сведения об общем и педагогическом стаже; сведения о наградах и поощрениях (при размещении по решению Оператора);

для внешних совместителей: дополнительно — сведения о должности по основному месту работы (только в объёме, необходимом для исполнения трудовых обязанностей и размещения обязательных сведений);

для лиц по договору ГПХ: фамилия, имя, отчество; сведения об уровне образования и квалификации; фотография (при согласии на распространение).

Сроки: сведения, размещаемые в силу закона (пп. 4, 4.1 ч. 2 ст. 29 Закона об образовании), — в период исполнения обязанностей и до истечения 10 рабочих дней после внесения изменений; сведения, размещаемые по решению Оператора, — в течение срока действия согласия на распространение, но не дольше периода трудовых отношений или действия договора ГПХ; при отзыве согласия — удаление в срок по ч. 2 ст. 9 Закона о персональных данных.

Цель 8. Регистрация участников, обеспечение доступа на площадку, формирование программы, выдача документов об участии, информационное сопровождение при организации и проведении форумов, конференций, семинаров, круглых столов и иных научно-практических и просветительских мероприятий.

Правовые основания: п. 5 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 26.07.2026) «О персональных данных» (исполнение договора, стороной либо выгодоприобретателем по которому является субъект персональных данных, либо принятие мер по заключению такого договора, в том числе публичной оферты на участие в мероприятии); пп. 1, 2 ч. 1 ст. 6 Закона о персональных данных (согласие субъекта персональных данных на обработку и на распространение персональных данных — при публикации сведений в материалах мероприятия, на сайте, в мобильном приложении, в списках участников, на бейджах); ст. 10.1 Закона о персональных данных (отдельное согласие на распространение персональных данных неопределённому кругу лиц — при размещении фамилии, имени, отчества, должности, места работы, фотографии в программе, на лендинге, в базе спикеров и т. п.); ст. 21 Федерального закона от 29.12.2012 № 273-ФЗ (ред. от 04.08.2026) «Об образовании в Российской Федерации» (в случае реализации мероприятия в рамках образовательной деятельности, в том числе как части дополнительной профессиональной программы).

Субъекты: физические лица, подавшие заявку на участие в мероприятии (слушатели, докладчики, модераторы, эксперты, представители СМИ, волонтёры), в том числе:

— штатные сотрудники организации;

— внешние участники (представители иных организаций, независимые специалисты);

— участники по направлению от работодателя;

— представители СМИ (на основании аккредитации);

— волонтёры;

Перечень персональных данных:

для регистрации и допуска на мероприятие: фамилия, имя, отчество; дата рождения; гражданство; данные документа, удостоверяющего личность (серия, номер, дата выдачи, кем

выдан — только для целей идентификации и контроля доступа); контактный телефон; адрес электронной почты; место работы и занимаемая должность; сведения об образовании и квалификации (по желанию участника, для формирования профиля участника);

для оформления документов об участии (удостоверение, сертификат, справка): фамилия, имя, отчество; данные документа, удостоверяющего личность; СНИЛС (при необходимости учёта в федеральной информационной системе ФИС ФРДО); сведения о документе об образовании (для внесения в удостоверение о повышении квалификации);

для публикации в материалах мероприятия (программа, сайт, мобильное приложение, бейдж): фамилия, имя, отчество; должность и место работы; сведения об учёной степени и учёном звании (при наличии); фотография (только при наличии отдельного согласия на распространение); тема выступления и тезисы доклада (обрабатываются с учётом прав на интеллектуальную собственность участника);

для организации логистики и сервиса (рассылка, кейтеринг, мерч): контактный телефон; адрес электронной почты; предпочтительный формат участия (очно/онлайн); особые потребности (доступная среда, диетические ограничения) — на добровольной основе.

Сроки: для целей регистрации, допуска и проведения мероприятия — в период подготовки и проведения мероприятия, а также в течение 30 календарных дней после его завершения (для выдачи документов, отчётов, закрывающих актов); для целей формирования и выдачи документов об обучении (удостоверений, сертификатов) и передачи сведений в ФИС ФРДО — в сроки, установленные Перечнем № 236, но не менее 50 лет для документов об образовании; для публикации сведений об участниках и спикерах на сайте и в материалах — в течение срока действия согласия на распространение персональных данных, но не дольше периода актуальности мероприятия (до 1 года после даты проведения); при отзыве согласия — удаление сведений в срок, установленный ч. 2 ст. 9 Закона о персональных данных; данные, используемые для рассылки и сервиса (телефон, адрес электронной почты, предпочтения), — до отзыва согласия субъектом либо истечения срока актуальности (не более 1 года после мероприятия), если иное прямо не указано в согласии.

Цель 9. Заключение и исполнение договоров об оказании гостиничных услуг и услуг иных средств размещения в отеле «Альфа» и общежитии.

Правовые основания: п. 3 ч. 1 ст. 6 Закона о персональных данных (договор найма жилого помещения, договор об оказании гостиничных услуг); постановление Правительства РФ от 27.11.2025 № 1912 «Об утверждении Правил предоставления гостиничных услуг и услуг иных средств размещения в Российской Федерации» (обязательный учёт постояльцев).

Субъекты: лица, заключившие договор о предоставлении жилого помещения в общежитии, и гости отеля «Альфа».

Перечень персональных данных: фамилия, имя, отчество; дата рождения; гражданство; данные документа, удостоверяющего личность; адрес регистрации; номер телефона; номер расчётного счёта (для расчётов по договору).

Сроки: период проживания; журнал регистрации — в течение 1 года после выбытия постояльца.

Цель 10. Обеспечение пропускного и внутриобъектового режима, антитеррористической защищённости объекта.

Правовые основания: п. 2 и 3 ч. 1 ст. 6 Закона о персональных данных; Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 25.05.2026) «О противодействии терроризму»; постановление Правительства РФ от 14.04.2017 № 447 (ред. от 03.09.2025) (требования к антитеррористической защищённости гостиниц и иных средств размещения); локальные акты о пропускном режиме.

Субъекты: работники Оператора, посетители.

Перечень персональных данных (общие): фамилия, имя, отчество; дата рождения; данные документа, удостоверяющего личность; номер телефона; должность и подразделение (для работников).

Сроки: период действия трудового договора (для работников); период нахождения на объекте (для посетителей).

Цель 11. Обеспечение безопасности объекта и сохранности имущества (видеонаблюдение).

Правовые основания: п. 4 ч. 1 ст. 6 Закона о персональных данных; ст. 86 ТК РФ (контроль количества и качества выполняемой работы, обеспечение сохранности имущества).

Субъекты: работники Оператора, посетители объекта и иные лица, попадающие в зону обзора камер видеонаблюдения.

Перечень персональных данных: изображения субъектов, полученные с помощью камер видеонаблюдения; записи журналов прохода.

Сроки: хранение записей — не более 30 суток, если иное не требуется для рассмотрения инцидента.

3.6. Категории субъектов персональных данных

— физические лица, состоящие с Оператором в трудовых отношениях;

— физические лица, уволившиеся из Оператора;

— физические лица, являющиеся кандидатами на работу;

— физические лица, состоящие с Оператором в гражданско-правовых отношениях;

—физические лица, являющиеся слушателями дополнительных профессиональных программ повышения квалификации и профессиональной переподготовки;

— физические лица, подавшие заявку на участие в форумах, конференциях, семинарах и иных мероприятиях Оператора;

— физические лица, заключившие договор о предоставлении жилого помещения для временного проживания в общежитии, и гости отеля «Альфа»;

— посетители объектов Оператора.

3.7. Перечни обрабатываемых персональных данных

— данные, полученные при осуществлении трудовых отношений;

— данные, полученные для осуществления отбора кандидатов на работу;

— данные, полученные при заключении и исполнении гражданско-правовых договоров;

—данные, полученные для оказания образовательных услуг по дополнительным профессиональным программам повышения квалификации и профессиональной переподготовки, включая сведения, вносимые в ФИС ФРДО;

—данные, полученные при регистрации участников мероприятий (форумов, конференций, семинаров) и при формировании документов об участии;

— данные, полученные для заключения договоров о предоставлении в пользование жилого помещения в общежитии;

— данные, полученные для заключения договоров об оказании гостиничных услуг в отеле «Альфа»;

— данные, полученные для осуществления пропускного режима;

— данные, полученные при обеспечении безопасности объекта (видеонаблюдение).

4. Хранение и уничтожение персональных данных

4.1. Хранение

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

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

4.1.3. Персональные данные, обрабатываемые с использованием средств автоматизации в разных целях, хранятся в разных папках (каталогах информационных систем).

4.1.4. Не допускается хранение и размещение документов, содержащих персональные данные, в открытых электронных каталогах (файлообменниках).

4.1.5. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели их обработки (ч. 1 ст. 21 Закона о персональных данных). Сроки хранения документов определены Перечнем № 236.

4.2. Уничтожение

4.2.1. Уничтожение документов (носителей), содержащих персональные данные, производится путём сожжения, дробления (измельчения), химического разложения, превращения в бесформенную массу или порошок. Для уничтожения бумажных документов допускается применение шредера.

4.2.2. Персональные данные на электронных носителях уничтожаются способами, исключающими возможность восстановления их содержания: путём стирания с последующей многократной перезаписью служебной информацией, программной очистки с многократной перезаписью, криптографического удаления либо физического уничтожения носителя.

4.2.3. Факт уничтожения персональных данных подтверждается документально актом об уничтожении носителей. Акты об уничтожении хранятся в соответствии с локальными нормативными актами Оператора и Перечнем № 236.

5. Защита персональных данных

5.1. В соответствии с требованиями нормативных документов Оператором создана система защиты персональных данных (СЗПД), состоящая из подсистем правовой, организационной и технической защиты.

5.2. Подсистема правовой защиты представляет собой комплекс правовых, организационно-распорядительных и нормативных документов, обеспечивающих создание, функционирование и совершенствование СЗПД.

5.3. Подсистема организационной защиты включает в себя организацию структуры управления СЗПД, разрешительной системы, защиты информации при работе с сотрудниками, партнёрами и сторонними лицами.

5.4. Подсистема технической защиты включает в себя комплекс технических, программных, программно-аппаратных средств, обеспечивающих защиту персональных данных.

5.5. Основными мерами защиты персональных данных, используемыми Оператором, являются:

5.5.1. Назначение лица, ответственного за организацию обработки персональных данных (ч. 1 ст. 22.1 Закона о персональных данных), которое осуществляет организацию обработки, обучение и инструктаж, внутренний контроль за соблюдением Оператором и его работниками требований к защите персональных данных.

5.5.2. Определение актуальных угроз безопасности персональных данных при их обработке в ИСПД и разработка мер и мероприятий по защите персональных данных (с применением требований приказа ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020); в случае вступления в силу нового приказа ФСТЭК — его положений).

5.5.3. Разработка политики в отношении обработки персональных данных и её публикация на сайте Оператора.

5.5.4. Установление правил доступа к персональным данным, обрабатываемым в ИСПД, а также обеспечение регистрации и учёта всех действий, совершаемых с персональными данными в ИСПД.

5.5.5. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

5.5.6. Применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

5.5.7. Применение антивирусного программного обеспечения с регулярно обновляемыми базами.

5.5.8. Соблюдение условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

5.5.9. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

5.5.10. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.5.11. Обучение работников Оператора, непосредственно осуществляющих обработку персональных данных, положениям законодательства РФ о персональных данных и внутренним документам Оператора (в порядке, установленном постановлением Правительства РФ от 24.12.2021 № 2464 (ред. от 30.06.2026), ст. 22.2 Закона о персональных данных).

5.5.12. Осуществление внутреннего контроля и аудита соответствия обработки персональных данных требованиям законодательства не реже одного раза в год.

6. Права субъектов персональных данных и обязанности Оператора

6.1. Основные права субъекта персональных данных

Субъект имеет право на доступ к его персональным данным и следующим сведениям (ч. 7 ст. 14 Закона о персональных данных):

— подтверждение факта обработки персональных данных Оператором;

— правовые основания и цели обработки персональных данных;

— цели и применяемые Оператором способы обработки персональных данных;

— 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;

— сроки обработки персональных данных, в том числе сроки их хранения;

— порядок осуществления субъектом персональных данных прав, предусмотренных Законом о персональных данных;

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

— обращение к Оператору и направление ему запросов;

— обжалование действий или бездействия Оператора в Роскомнадзор или в суд.

6.2. Обязанности Оператора

— при сборе персональных данных предоставить информацию об их обработке;

— в случаях, если персональные данные получены не от субъекта, уведомить субъекта;

— при отказе в предоставлении персональных данных субъекту разъяснить последствия такого отказа;

— опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику в отношении обработки персональных данных, и к сведениям о реализуемых требованиях к защите персональных данных;

— принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных;

— давать ответы на запросы и обращения субъектов персональных данных, их представителей и уполномоченного органа по защите прав субъектов персональных данных;

— уведомить Роскомнадзор о намерении осуществлять обработку персональных данных и актуализировать сведения в уведомлении (ч. 7 ст. 22 Закона о персональных данных); за непредставление уведомления предусмотрена административная ответственность по ч. 10 ст. 13.11 КоАП РФ.

7. Обращения и запросы субъектов. Актуализация, уточнение, удаление и уничтожение персональных данных

7.1. Подтверждение факта обработки персональных данных Оператором, правовые основания и цели обработки, а также иные сведения, указанные в ч. 7 ст. 14 Закона о персональных данных, предоставляются субъекту персональных данных или его представителю при обращении либо при получении запроса субъекта персональных данных или его представителя (ст. 20 Закона о персональных данных).

В предоставляемые сведения не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, когда имеются законные основания для раскрытия таких персональных данных.

Запрос должен содержать:

— номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе;

— сведения, подтверждающие участие субъекта в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором;

— подпись субъекта персональных данных или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Ответ на запрос предоставляется в течение 10 рабочих дней; срок может быть продлён не более чем на 5 рабочих дней с уведомлением субъекта (ст. 20 Закона о персональных данных).

Если в обращении (запросе) не отражены все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, ему направляется мотивированный отказ.

Право субъекта на доступ к его персональным данным может быть ограничено в соответствии с ч. 8 ст. 14 Закона о персональных данных, в том числе если доступ субъекта к его персональным данным нарушает права и законные интересы третьих лиц.

7.2. В случае выявления неточных персональных данных при обращении субъекта или его представителя либо по запросу Роскомнадзора Оператор осуществляет блокирование персональных данных, относящихся к этому субъекту, с момента такого обращения или получения запроса на период проверки, если блокирование не нарушает права и законные интересы субъекта или третьих лиц. В случае подтверждения факта неточности персональных данных Оператор уточняет их в течение семи рабочих дней со дня представления сведений и снимает блокирование (ч. 4 ст. 21 Закона о персональных данных).

7.3. В случае выявления неправомерной обработки персональных данных Оператор в срок, не превышающий трёх рабочих дней со дня выявления неправомерной обработки, обязан прекратить неправомерную обработку. Если субъектом не достигнута цель обработки, Оператор обязан уничтожить персональные данные или обеспечить их обезличивание в срок, не превышающий тридцати дней со дня выявления неправомерной обработки. Если срок устранения нарушений превышает указанные сроки, Оператор осуществляет блокирование персональных данных (ч. 3 ст. 21 Закона о персональных данных, в редакции Федерального закона от 30.12.2021 № 474-ФЗ).

7.4. При достижении целей обработки персональных данных, а также в случае отзыва субъектом согласия на их обработку персональные данные подлежат уничтожению, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, другим соглашением между Оператором и субъектом либо федеральными законами, на основании которых Оператор вправе осуществлять обработку без согласия субъекта.

8. Реагирование на инциденты (утечку) персональных данных

8.1. В случае выявления факта неправомерной передачи персональных данных (утечки) либо угрозы такого факта Оператор обязан уведомить Роскомнадзор об этом факте в течение 24 часов, а о результатах внутреннего расследования — в течение 72 часов с момента выявления (ч. 3.1 ст. 21 Закона о персональных данных). Уведомление направляется через портал Роскомнадзора (pd.rkn.gov.ru).

8.2. Оператор организует внутреннее расследование инцидента: фиксирует обстоятельства, объём и состав утёкших персональных данных, принимает меры по устранению причин и минимизации последствий, при необходимости уведомляет субъектов персональных данных и правоохранительные органы.

8.3. За неуведомление о факте неправомерной передачи (утечки) персональных данных предусмотрена административная ответственность по ч. 11 ст. 13.11 КоАП РФ (размер санкции — в актуальной редакции КоАП РФ).

9. Трансграничная передача персональных данных

9.1. Трансграничная передача персональных данных осуществляется в соответствии со ст. 12 Закона о персональных данных при условии соблюдения требований, установленных законодательством.

9.2. До начала осуществления трансграничной передачи Оператор направляет в Роскомнадзор отдельное уведомление о намерении осуществлять трансграничную передачу персональных данных (ч. 8 ст. 22 Закона о персональных данных).

9.3. В отношении государств, включённых Роскомнадзором в перечень иностранных государств, обеспечивающих надлежащую защиту прав субъектов персональных данных (утв. приказом Роскомнадзора от 16.09.2026 № 253), передача осуществляется после направления уведомления. В отношении иных иностранных государств передача осуществляется по истечении десяти рабочих дней с даты направления уведомления, если Роскомнадзор не примет решение о её запрете.

10. Заключительные положения

10.1. Ответственность за нарушение требований законодательства Российской Федерации и нормативных документов ФГБОУ ДПО СПИУПТ в области персональных данных определяется в соответствии с законодательством Российской Федерации, в том числе ст. 13.11 КоАП РФ (нарушения правил обработки, включая утечки и невыполнение обязанностей по уведомлению Роскомнадзора) и ст. 272.1 Уголовного кодекса РФ (незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, доступ к которой охраняется законом, информации о частной жизни физического лица либо информации, содержащейся в переписке, телефонных переговорах, почтовых, телеграфных или иных сообщениях физического лица).

10.2. Настоящая Политика вступает в силу с момента утверждения и действует бессрочно до принятия новой Политики.

10.3. Все изменения и дополнения к настоящей Политике утверждаются ректором ФГБОУ ДПО СПИУПТ.