УТВЕРЖДАЮ
директор ГБУ ЛО «ИЦОКО»
_____ И.Н. Грозная
Приказ 21 февраля 2020 г. №20

ПОЛОЖЕНИЕ

об обработке и защите персональных данных
в государственном бюджетном учреждении Ленинградской области
«Информационный центр оценки качества образования»

1. Общие положения

1.1. Положение об обработке и защите персональных данных (далее - Положение) устанавливает порядок и условия получения, обработки, хранения, передачи, защиты и любого другого использования персональных данных в государственном бюджетном учреждении Ленинградской области «Информационный центр оценки качества образования» (далее - Учреждение) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон), главой 14 Трудового кодекса Российской Федерации, Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 №687, Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, утвержденными постановлением Правительства Российской Федерации от 06.07.2008 №512, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18.02.2013 №21, Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого уровня защищенности, утвержденными приказом ФСБ России от 10.07.2014 №378, Кодексом Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ.

1.2. Цель настоящего Положения - обеспечение защиты законных интересов, прав и свобод работников Учреждения, членов их семей, представителей сторонних организаций, физических лиц, выполняющих работы (оказывающих услуги) в интересах Учреждения на основании договоров, представителей федеральных органов исполнительной власти, комитета общего и профессионального образования Ленинградской области, органов местного самоуправления, осуществляющих управление в сфере образования, образовательных организаций Ленинградской области, потребителей по вопросам, относящимся к компетенции Учреждения, участников государственной итоговой аттестации (далее - ГИА), посетителей Учреждения при обработке их персональных данных.

Положение является документом, определяющим политику Учреждения в отношении обработки персональных данных и содержащим сведения о реализуемых требованиях к их защите.

1.3. Согласно Закону, под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

К персональным данным относятся:

фамилия, имя, отчество; дата и место рождения; пол; паспортные данные; адрес проживания (регистрации); семейное положение, социальное, имущественное положение; должность (профессия, специальность); страховой номер индивидуального лицевого счета; индивидуальный номер налогоплательщика (ИНН); доходы; сведения об образовании, квалификации, профессиональной подготовке, повышении квалификации; содержание трудового договора; другие сведения, в том числе для участников ГИА, указанные в Приложении №3 к Положению.

1.4. К документам, содержащим персональные данные, относятся:

паспорт (иной документ, удостоверяющий личность); анкеты; заявления; трудовые книжки; приказы Учреждения по личному составу; страховое свидетельство обязательного пенсионного страхования; свидетельство о присвоении ИНН; документы воинского учета; личные дела, карточки, журналы, книги, содержащие данные по работникам; документы об образовании, о квалификации или наличии специальных знаний; документы, содержащие информацию о повышении квалификации и переподготовке работников, служебных расследованиях; документы бухгалтерского учета, содержащие информацию о расчетах с работниками Учреждения, физическими лицами, заключившими с Учреждением договоры гражданско-правового характера; трудовые договоры; рекомендации, характеристики; медицинские документы, в том числе справки, листки нетрудоспособности; проездные документы, приобретаемые Учреждения для командирования; контрольно-измерительные материалы участников ГИА; иные документы, содержащие персональные данные.

1.5. Учреждение является оператором персональных данных, самостоятельно или совместно с другими лицами осуществляющим обработку персональных данных, а также определяющим цели обработки персональных данных, состав подлежащих обработке персональных данных и действия (операции), совершаемые с персональными данными (далее - Оператор).

Оператор получает необходимые для обработки персональные данные непосредственно от субъектов персональных данных.

Во исполнение распоряжения Правительства Ленинградской области от 16 января 2007 года № 6-р Оператор получает необходимые для обработки персональные данные из пунктов проведения экзаменов и муниципальных образований на территории Ленинградской области, из Федерального государственного бюджетного учреждения «Федеральный центр тестирования» (далее - ФЦТ).

Получение персональных данных иными способами запрещено.

1.6. Субъекты персональных данных, предоставившие свои персональные данные Оператору, вправе:

1.6.1. Получать от Оператора информацию, предусмотренную пунктом 7 ст.14 Закона, в том числе содержащую:

-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;
-обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
-сроки обработки персональных данных, в том числе сроки их хранения;
-порядок осуществления субъектом персональных данных прав, предусмотренных Законом;
-информацию об осуществленной передаче данных;
-наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
-иные сведения, предусмотренные Законом или другими федеральными законами.

1.6.2. Требовать внесения необходимых изменений, уничтожения или блокирования соответствующих персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

1.6.3. Требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

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

2. Основные понятия и определения

Обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без использования таких средств, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (далее - ИСПДн) -совокупность

содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Угроза безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные неправомерные действия при их обработке в ИСПДн.

Актуальная угроза - угроза, которая может быть реализована в ИСПДн и представляет опасность для персональных данных.

3. Цели обработки персональных данных

3.1. Обработка персональных данных Оператором осуществляется для достижения конкретных, заранее определенных и законных целей, в соответствии с законодательными, нормативными правовыми актами Российской Федерации и учредительными документами Учреждения.

3.2. В соответствии со статьей 65 Трудового кодекса Российской Федерации, подпунктами 2, 5 пункта 1 статьи 6 Закона, статьей 226 Налогового кодекса Российской Федерации Оператором осуществляется обработка персональных данных работников Учреждения (в том числе автоматизированная) в целях:

-ведения административно-кадровой работы;

-реализации социальной политики Учреждения;

-осуществления мобилизационной подготовки, ведения воинского учёта;

-ведения бухгалтерского учета;

-содействия работнику в выполнении должностных обязанностей, обучении и должностном росте, обеспечения личной безопасности работника, учета результатов исполнения им должностных обязанностей;

-обеспечения пропускного режима и сохранности имущества Учреждения;

-информационного обеспечения деятельности Учреждения.

3.3. В соответствии с Гражданским кодексом Российской Федерации в целях организации работ по оказанию услуг Учреждению физическими лицами, выполнения функций налогового агента, ведения бухгалтерского учета и учета результатов оказания услуг Оператор осуществляет обработку (в том числе автоматизированную) персональных данных физических лиц (субъектов персональных данных), заключивших с Учреждением договоры гражданско-правового характера.

3.4. В целях подбора персонала Учреждение осуществляет обработку персональных данных (в том числе автоматизированную) кандидатов на замещение вакантных должностей Учреждения.

3.5. В целях обеспечения пропуска на территорию Учреждения Оператор осуществляет обработку (в том числе автоматизированную) персональных данных посетителей, представителей муниципальных органов управления образованием, лиц, выполняющих работы (оказывающих услуги) в интересах Учреждения на основании договоров.

3.6. В соответствии с Распоряжением правительства Ленинградской области от 16 января 2007 года №6-р Учреждение осуществляет обработку и передачу персональных

данных лиц, участвующих в ГИА, в целях:
-организационно - технологического сопровождения государственной итоговой аттестации обучающихся в образовательных организациях Ленинградской области освоивших образовательные программы основного общего и среднего общего образования;
-организационно - технологического сопровождения контрольно-педагогических измерений образовательной деятельности, мероприятий мониторингов качества образования и контрольно-надзорных мероприятий на территории Ленинградской области;
-технической поддержки информационных систем, обеспечивающих государственную итоговую аттестацию обучающихся.

3.7. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.8. По достижении целей обработки персональные данные субъектов персональных данных должны быть уничтожены или обезличены, или переданы в архив.

4. Порядок организации и общие положения по обработке персональных данных

4.1. Приказом по Учреждению назначается работник, ответственный за организацию обработки персональных данных (далее - ответственный за организацию обработки персональных данных). Ответственный за организацию обработки персональных данных получает указания непосредственно от директора Учреждения и подотчетен ему.

4.2. Ответственный за организацию обработки персональных данных обязан:
-осуществлять внутренний контроль за соблюдением в Учреждении законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
-организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;
-организовывать доведение до сведения работников Учреждения положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

4.3. Обработка персональных данных в Учреждении осуществляется в смешанном режиме, как с использованием средств автоматизации, так и без использования средств автоматизации.

4.4. Обработку персональных данных, в объеме, необходимом для выполнения должностной инструкции, имеют право вести уполномоченные работники Учреждения, давшие обязательство о недопущении несанкционированной передачи и распространения персональных данных (приложение № 2 к Положению).

Перечень должностей, замещаемых работниками, имеющими право обработки персональных данных, формируется и поддерживается в актуальном состоянии.

4.5. Уполномоченные работники Учреждения, обрабатывающие персональные данные в соответствии с должностной инструкцией, обязаны соблюдать следующие требования:

4.5.1. На условиях, предусмотренных статьей 6 Закона, обработка должна осуществляться с письменного согласия субъекта персональных данных на обработку его персональных данных (далее - Согласие), которое действует в течение срока, определенного в Согласии. Форма Согласия представлены в приложении №1 к Положению.

4.5.2. Запрещается получать, обрабатывать и приобщать к делу субъекта персональных данных сведения о его политических, религиозных и иных убеждениях,

частной жизни, членстве в общественных объединениях.

4.5.3. Объем и характер обрабатываемых персональных данных, способы их обработки должны соответствовать целям обработки персональных данных. В случае увеличения перечня обрабатываемых персональных данных и/или изменения перечня действий с персональными данными, Оператор имеет право на оформление нового Согласия, учитывающего указанные изменения.

4.5.4. При принятии решений, затрагивающих интересы субъекта персональных данных, запрещено основываться на решениях, принятых исключительно в результате автоматизированной обработки персональных данных без письменного согласия субъекта персональных данных.

4.5.5. Создание видеоизображений в Учреждении ведется только с целью контроля соблюдения законности и правопорядка, а также предотвращения противоправных действий, экстремистских проявлений и террористических актов. В случае необходимости видеоматериалы могут передаваться в правоохранительные органы.

4.5.6. Передача персональных данных не допускается без письменного согласия субъекта персональных данных, за исключением случаев, установленных законодательством Российской Федерации.

4.5.7. При заключении Учреждением договоров гражданско-правового характера, по условиям которых предусмотрено предоставление персональных данных, в договоры должны быть включены обязательства сторон о выполнении требований Федерального закона «О персональных данных», об обеспечении конфиденциальности полученных персональных данных и об использовании их только в целях, предусмотренных условиями договоров.

4.5.8. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться в сроки, определенные законодательством Российской Федерации, нормативными документами правительства Ленинградской области или договором, стороной которого является субъект персональных данных. Если срок хранения не установлен, персональные данные могут храниться не дольше, чем этого требуют цели обработки. По истечении срока хранения персональные данные подлежат уничтожению либо обезличиванию.

4.5.9. Персональные данные могут считаться обезличенными в случаях:

-исключения фамилии, имени и отчества из обрабатываемых реквизитов персональных данных физического лица;

-обработки фамилии, имени и отчества без прочих реквизитов персональных данных физического лица.

5. Порядок обработки персональных данных без использования средств автоматизации

5.1. Обработка персональных данных без использования средств автоматизации обеспечивает достоверность и актуальность персональных данных и включает обработку персональных данных на материальных носителях, указанных в п. 1.4 Положения.

5.2. Субъект персональных данных предоставляет Оператору достоверные сведения о себе и оформляет письменное согласие на обработку его персональных данных. Уполномоченный работник Учреждения при обработке персональных данных проверяет их достоверность, сверяя представленные данные с имеющимися у субъекта персональных данных документами. Предоставление подложных документов при заключении договора является основанием расторжения трудового договора (пункт 11 части первой статьи 81

Трудового кодекса Российской Федерации), отказа в заключении трудового или иного договора.

5.3. При обработке персональных данных без использования средств автоматизации уполномоченными работниками не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

5.4. При ознакомлении субъекта персональных данных с документами, содержащими его персональные данные и персональные данные других субъектов персональных данных, не должны нарушаться законные права и интересы каждого из них. При этом субъекту персональных данных обеспечивается доступ только к той части документа, где содержатся его персональные данные.

5.5. Уничтожение или обезличивание персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Черновики документов, испорченные листы, неподписанные проекты документов уничтожаются путем измельчения или другим путем, исключающим восстановление документов.

5.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

5.7. Согласия на обработку персональных данных работников Учреждения (в том числе работающих по срочным договорам) и членов их семей хранятся в личных делах работников Учреждения.

5.8. Доступ работников Учреждения к содержащим персональные данные материальным носителям осуществляется в соответствии с Регламентом предоставления доступа работникам Учреждения к персональным данным, хранящимся на бумажных носителях (приложение №4 к Положению).

5.9. Персональные данные на материальных носителях хранятся таким образом, чтобы исключить их несанкционированное использование (в металлических шкафах или сейфах).

6. Порядок автоматизированной обработки персональных данных

6.1. Для автоматизированной обработки персональных данных в Учреждении используются ИСПДн различного функционального назначения.

6.2. Перечень ИСПДн и персональных данных, обрабатываемых в них, указан в приложениях №4-5 к Положению.

6.3. Персональные данные из ИСПДн могут быть предоставлены: уполномоченным работникам Учреждения в соответствии с их должностной инструкцией в:

-региональные органы исполнительной власти в порядке, установленном законодательством Российской Федерации;

-ФЦТ, в пункты проведения экзаменов на территории Ленинградской области в порядке и объеме, определенном Комитетом общего и профессионального образования Ленинградской области;

-страховые организации, государственные пенсионные фонды, организации, оказывающие Учреждению банковские и другие финансовые услуги, учебные заведения, оказывающие услуги по обучению, переподготовке и повышению квалификации работников Учреждения, операторам связи, аккредитованные удостоверяющие центры, военные комиссариаты, органы местного самоуправления, в порядке и объеме, определенном законодательными и

нормативными правовыми актами Российской Федерации, согласием субъекта персональных данных, соответствующими договорами.

6.4. В целях информационного обеспечения в Учреждении могут создаваться общедоступные источники персональных данных (в том числе веб-сайт). В общедоступные источники персональных данных с письменного Согласия работников Учреждения могут включаться их фамилия, имя, отчество, занимаемая должность, год и место рождения, номера телефонов, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных для размещения в общедоступных источниках персональных данных.

6.5. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по письменному заявлению субъекта персональных данных.

7. Обеспечение безопасности персональных данных

7.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы безопасности персональных данных.

7.2. Организация работы по обеспечению безопасности персональных данных в Учреждении возлагается на ответственного за организацию обработки персональных данных.

7.3. Безопасность персональных данных обеспечивается:

7.3.1. Определением актуальных угроз безопасности персональных данных и разработкой частной модели угроз безопасности персональных данных при их обработке в ИСПДн.

7.3.2. Применением определенных федеральным законодательством организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн.

7.3.3. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

7.3.4. Оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода ИСПДн в эксплуатацию.

7.3.5. Оценкой эффективности реализованных в системе защиты персональных данных мер по обеспечению безопасности персональных данных. Оценка эффективности реализованных мер проводится не реже одного раза в три года.

7.3.6. Учетом машинных носителей персональных данных в соответствии с нормативными документами Учреждения.

7.3.7. Обнаружением фактов несанкционированного доступа к персональным данным и принятием мер.

7.3.8. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

7.3.9. Установлением правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн.

7.4. В случае если персональные данные работников Учреждения и субъектов персональных данных, не являющихся работниками Учреждения, предоставивших свои персональные данные Оператору, являются общедоступными на основании оформления

Согласия или федерального законодательства, может быть принято решение о неактуальности угроз конфиденциальности таких данных. В этих случаях персональные данные указанных субъектов могут передаваться по открытым каналам связи, в том числе через информационно-телекоммуникационные сети общего пользования.

8. Ответственность за организацию обработки персональных данных

8.1. Руководители подразделений Учреждения, чьи работники имеют право обрабатывать персональные данные, обеспечивают выполнение правовых, организационных и технических мер по защите персональных данных, предусмотренных законодательными и иными нормативными актами Российской Федерации в части, их касающейся, и несут ответственность:

8.1.1. Директор Учреждения за:

-организацию оформления согласий на обработку персональных данных работниками Учреждения;

-организацию оформления работниками Учреждения обязательств о недопущении несанкционированной передачи и распространения персональных данных;

-организацию оформления согласий на обработку персональных данных физическими лицами, заключающими с Учреждения договоры гражданско-правового характера. Оформленное согласие хранится вместе с оригиналом договора.

-обработку поступивших в Учреждение обращений и запросов субъектов персональных данных, подготовку ответов на указанные обращения и запросы.

8.1.2. Отдел информатизации, средств телекоммуникаций и сервисного обслуживания за:

-ознакомление работников Учреждения с требованиями нормативных правовых актов Российской Федерации в области персональных данных;

-планирование, организацию и контроль выполнения мероприятий по обеспечению безопасности персональных данных;

-разработку организационно-распорядительных документов в области персональных данных;

-разработку частных моделей угроз безопасности персональных данных при их обработке в ИСПДн;

-методическое руководство в вопросах обеспечения безопасности персональных данных;

-обеспечение контроля выполнения работниками Учреждения требований по защите персональных данных при их обработке на материальных носителях;

-разработку и реализацию требований по обеспечению безопасности персональных данных при создании и эксплуатации ИСПДн;

-эксплуатацию, сопровождение, адаптацию, развитие и вывод из эксплуатации ИСПДн;

-реализацию мер по обезличиванию и/или уничтожению персональных данных, обрабатываемых в ИСПДн;

-организацию защиты персональных данных с использованием средств криптографической защиты информации при принятии соответствующего решения;

-контроль состояния антивирусной защиты ИСПДн;

-информирование руководства учреждения о всех выявленных нарушениях безопасности информации (фактах или попытках несанкционированного доступа);

-подготовку и направление заявок на классификацию ИСПДн, вводимых в эксплуатацию в интересах Учреждения.

8.2. Ответственными за соблюдение требований по защите персональных данных при их автоматизированной обработке являются:

-начальник отделов, в интересах которых эксплуатируются ИСПДн,
-уполномоченные работники, непосредственно обрабатывающие персональные данные в ИСПДн,
-инженерно-технический персонал, имеющий доступ к ИСПДн с целью обеспечения их устойчивого функционирования, что отражается в должностных инструкциях указанных лиц;

8.3. Лица, указанные в подразделе 8.2. настоящего Положения, осуществляют обработку персональных данных в соответствии с требованиями Закона и иных нормативных правовых актов Российской Федерации в сфере защиты персональных данных, а также несут ответственность за нарушение законодательства Российской Федерации в области персональных данных.

9. Ответственность за нарушение норм, регулирующих обработку персональных данных

9.1. Учреждение несет ответственность за обеспечение безопасности персональных данных, которые находятся в его распоряжении, и закрепляет персональную ответственность работников за соблюдение установленного режима конфиденциальности в отношении персональных данных.

9.2. Работники Учреждения, осуществляющие обработку персональных данных, несут персональную ответственность за соблюдение установленных требований по обеспечении безопасности персональных данных.

9.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут ответственность, предусмотренную законодательством Российской Федерации.