УТВЕРЖДАЮ
начальник МУ «УО местной
администрации Баксанского
муниципального района»
_____ / Абрегова Т.К.
«29» декабря 2017 г.

Политика обработки персональных данных МУ «УО местной администрации Баксанского муниципального района»

г. Баксан
2017г.

1.Общие положения

1.1. Настоящая Политика об обработке персональных данных (далее – Политика):

– является основополагающим внутренним документом МУ «УО местной администрации Баксанского муниципального района» (далее – Учреждение), регулирующим вопросы обработки персональных данных;

– разработана в целях обеспечения соответствия с законодательством Российской Федерации обработки, хранения и защиты ПДн сотрудников, граждан и депутатов;

– раскрывает основные категории персональных данных, обрабатываемых Учреждением, цели, способы и принципы обработки Учреждения, права и обязанности Учреждения при обработке персональных данных, права субъектов персональных данных, а также перечень мер, применяемых Учреждением в целях обеспечения безопасности персональных данных при их обработке;

– предназначена для сотрудников Учреждения, осуществляющих обработку персональных данных в целях непосредственной реализации ими закрепленных в Политике принципов, а также является информационным ресурсом для субъектов персональных данных, позволяющим определить концептуальные основы деятельности Учреждения при обработке персональных данных.

2.Источники нормативного правовогорегулирования вопросов обработки персональных данных

2.1.Политика Учреждения в области обработки персональных данных определяется на основании следующих нормативных правовых актов РФ:

– Конституции Российской Федерации;

– Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

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

– Совместный приказ от 13 февраля 2008 года ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи России № 20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

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

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

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

– Приказ ФСТЭК России от 5.02.2010 № 58,зарегистрированный в Минюсте России 19.02.2010 № 16456 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».

– Постановление Правительства РФ от 27.01.2012 № 36 Об утверждении правил формирования и ведения ФИС обеспечения проведения ЕГЭ и приема в ВУЗы и ССУЗы и РИС обеспечения проведения ЕГЭ

2.2.Во исполнение настоящей Политики в Учреждении приказами утверждаются следующие локальные нормативные правовые акты:

– Инструкция Специалиста по защите информации информационных систем персональных данных;

– Инструкция по действиям пользователей информационных систем персональных данных в нештатных ситуациях;

– Инструкция по организации антивирусной защитыинформационных систем персональных данных;

– Инструкция по порядку проведения проверок состояния защиты персональных данных;

– План внутренних проверок состояния защиты персональных данных;

– Инструкция Пользователя информационных систем персональных данных;

– Перечень персональных данных, обрабатываемых в Учреждении;

– План мероприятий по защите персональных данных;

– Положение о порядке организации и проведению работ по обработке и защите персональных данных, обрабатываемых в информационных системах персональных данныхУчреждения;

– Акт классификации информационных систем персональных данных Учреждения;

– Модель угроз и нарушителябезопасности персональных данныхинформационных систем персональных данныхУчреждения;

– и иныелокальныедокументыУчреждения,принимаемыевоисполнениетребований действующихнормативныхправовыхактовРФвобластиобработкиперсональных данных.

3.Основные термины и понятия ,используемые в локальных документахУчреждения, принимаемых по вопросуобработкиперсональныхданных

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн), в том числе его фамилия, имя, отчество, год, месяц, дата и

место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в Учреждении локальными актами Учреждения.

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

Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

Предоставление персональных данных – действия, направленные на раскрытие ПДн определенному кругу.

Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

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

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

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

Информационная система персональных данных – информационная система, представляющая собой совокупность содержащихся в базе данных ПДн и их обработку, информационных технологий и технических средств.

Конфиденциальная информация – информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и

представляет собой коммерческую, служебную или личную тайны, охраняющиеся её владельцем.

Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

4.Общие условия обработки персональных данных

4.1 Обработка ПДн в Учреждении осуществляется на основе следующих принципов:

4.1.1 Законности и справедливости обработки ПДн.

4.1.2 Законности целей и способов обработки ПДн и добросовестности.

4.1.3 Соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Учреждения.

4.1.4 Соответствия содержания и объема обрабатываемых ПДн целям обработки ПДн.

4.1.5 Достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн.

4.1.6 Недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

4.1.7 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.8 Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.1.9 Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.1.10Субъект ПДн является собственником своих ПДн и самостоятельно решает вопрос передачи Учреждению своих ПДн.

4.1.11Держателем ПДн является Учреждение, которому субъект ПДн передает во владение свои ПДн. Учреждение выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

4.1.12 Комплекс мер по защите ПДн направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности

ПДн и обеспечивает безопасность информации в процессе деятельностиУчреждения.

4.1.13 Учреждение при обработке ПДн обязано принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн.

4.1.14 Мероприятия по защите ПДн определяются Положением, приказами, инструкциями и другими внутренними документами Учреждения.

4.2 Для защиты ПДн в Учреждении применяются следующие принципы и правила:

4.2.1 Ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей ПДн.

4.2.2 Строгое избирательное и обоснованное распределение документов и информации между сотрудниками.

4.2.3 Рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации.

4.2.4 Знание сотрудниками требований нормативно-методических документов по защите ПДн.

4.2.5 Распределение персональной ответственности между сотрудниками, участвующими в обработке ПДн, за выполнение требований по обеспечению безопасности ПДн.

4.2.6 Установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности ПДн при работе с конфиденциальными документами и базами данных.

4.2.7 Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

4.2.8 Исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка ПДн и находится соответствующая вычислительная техника.

4.2.9 Организация порядка уничтожения персональных данных.

4.2.10 Своевременное выявление нарушений требований разрешительной системы доступа.

4.2.11 Воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

4.2.12 Регулярное обучение работников по вопросам, связанным с обеспечением безопасности ПДн.

4.2.13 Ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся ПДн.

4.2.14 Создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией.

4.2.15 Резервирование защищаемых данных (создание резервных копий).

4.3 Цели обработки персональных данных:

4.3.1. Исполнение требований законодательства и договора с абитуриентом

4.4 Правовое основание обработки персональных данных:

4.4.1 Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

4.4.2 Федеральное законодательство.