**Государственное автономное образовательное учреждение
дополнительного профессионального образования
Владимирской области
«Владимирский институт развития образования имени Л.И. Новиковой»**

ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ: НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ

Методические рекомендации

Владимир, 2023

УДК 342.7
ББК 67.400.7
О 64

Печатается по решению редакционно-издательского совета ГАОУ ДПО ВО ВИРО

Автор-составитель

Соловьев Михаил Юрьевич,
кандидат экономических наук, профессор кафедры педагогического менеджмента ГАОУ ДПО ВО «Владимирский институт развития образования имени Л.И. Новиковой».

Организация работы по защите персональных данных при их обработке в образовательной организации: нормативно-правовое регулирование: методические рекомендации / авт.-сост. М.Ю. Соловьев. – Владимир: ГАОУ ДПО ВО ВИРО, 2023. – 68 с.

Методические рекомендации посвящены вопросам организации работы по защите персональных данных при их обработке в образовательной организации. Материалы пособия содержат основные понятия, используемые в практической деятельности руководителей образовательных организаций и лиц, ответственных за работу с персональными данными работников и обучающихся в образовательной организации, раскрывают общие подходы, включая виды персональных данных, способы, принципы и условия их обработки, описывают функции и обязанности оператора персональных данных при этом, возможные процедуры, механизмы, управленческие решения, меры организационно-правового обеспечения безопасности персональных данных при их обработке, хранении и передаче на локальном уровне.

ОГЛАВЛЕНИЕ

Глава 1.
ВВЕДЕНИЕ И ОСНОВНЫЕ ИСПОЛЬЗУЕМЫЕ ПОНЯТИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящие рекомендации разработаны в соответствии с действующим законодательством РФ в целях оказания методической помощи руководителям государственных и муниципальных образовательных организаций и лицам, ответственным за работу с персональными данными работников и обучающихся в образовательной организации.

Материалы пособия содержат основные понятия, используемые в практической деятельности руководителей и лиц, ответственных за работу с персональными данными в образовательной организации, раскрывают общие подходы, включая виды персональных данных, способы, принципы и условия их обработки, описывают функции и обязанности оператора персональных данных при этом, возможные процедуры, механизмы, управленческие решения, меры организационно-правового обеспечения безопасности персональных данных при их обработке, хранении и передаче на локальном уровне.

Рекомендации излагают общие подходы, принципы, требования и условия обработки персональных данных, описывают функции и обязанности оператора при обработке, получении и хранении персональных данных, меры ответственности образовательных организаций и их должностных лиц за нарушение законодательства о персональных данных.

В методических материалах раскрываются особенности обработки и защиты персональных данных работников и обучающихся образовательной организации, порядок разработки и принятия локальных актов по защите персональных данных, содержание их структурных элементов и прилагаются макеты некоторых организационно-распорядительных документов.

В рекомендациях используются следующие понятия и определения.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной

системы, в том числе по обработке информации, содержащейся в ее базах данных.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом.

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), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Администратор [системный, безопасности] – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы (администратор системный) и (или) ее системы защиты информации (администратор безопасности) в соответствии с установленной ролью.

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

Средства автоматизации – это программные и аппаратные средства, которые предназначены для автоматизации различных процессов в бизнесе.

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.

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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Обладатель информации – «собственник» – «титульный ее владелец» – лицо правомочное в отношении конкретной информации решать вопрос о ее получении другими лицами и о способах ее использования как им самим, так и другими лицами, а также вправе совершать в отношении этой информации действия, являющиеся прерогативой обладателя информации.

Базовый набор мер защиты информации **–** минимальный набор мер защиты информации, установленный для соответствующего класса защищенности информационной системы.

Защищенные линии связи **–** линии (каналы) связи, при передаче информации по которым обеспечивается требуемый уровень ее защищенности (конфиденциальность, целостность и (или) доступность информации).

Конфиденциальность информации **–** свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Локальный нормативный акт – правовой распорядительный документ, издаваемый руководителем организации в пределах своей компетенции в соответствии с законами, иными нормативными правовыми актами, коллективным договором, соглашениями.

Автоматизированная обработка персональных данных **–** обработка персональных данных с помощью средств вычислительной техники.

Деобезличивание **–** действия, в результате которых обезличенные данные принимают вид, позволяющий определить их принадлежность конкретному субъекту персональных данных, то есть становятся персональными данными.

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

Обезличенные данные **–** это данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации.

Обработка обезличенных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации, с обезличенными данными, без применения их предварительного деобезличивания.

Атрибут персональных данных субъекта – элемент структуры персональных данных (параметр персональных данных). Атрибут имеет название и может иметь множество возможных количественных и

качественных значений применительно к конкретным субъектам персональных данных.

Атрибут обезличенных данных субъекта – элемент структуры обезличенных данных (параметр обезличенных данных). Атрибут имеет название и может иметь множество возможных количественных и качественных значений.

Семантика атрибута персональных данных – смысловое значение названия атрибута, обозначения персональных данных.

Семантика атрибута, обезличенных данных – смысловое значение названия атрибута, обозначения обезличенных данных.

Средство криптографической защиты информации (СКЗИ) – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Глава 2.
ОБЩИЕ ПОДХОДЫ, ПРИНЦИПЫ, ТРЕБОВАНИЯ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общие подходы к обработке персональных данных

Общие подходы к обработке персональных данных установлены законодательством Российской Федерации и международными правовыми нормами.

Основополагающими документами, регулирующими работу с персональными данными, являются:

Конституция Российской Федерации, устанавливает в статье 24 запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия, но в то же время предоставляет в соответствии со статьей 29 право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Согласно статье 71 Конституции РФ вопросы, относящиеся к информации, информационным технологиям и связи, обеспечению безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных отнесены к ведению Российской Федерации.

В Российской Федерации при обработке персональных данных учитываются положения *Конвенции о защите физических лиц при автоматизированной обработке персональных данных*, принятой в Страсбурге 28.01.1981. Согласно данному документу каждому физическому лицу гарантируется право на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных. Персональные данные, подвергающиеся автоматизированной обработке, собираются и обрабатываются на справедливой и законной основе, хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями, являются адекватными, точными и обновляются при необходимости. Для защиты персональных данных, хранящихся в автоматизированных файлах данных, принимаются надлежащие меры безопасности, направленные на предотвращение их случайного или несанкционированного уничтожения или случайной потери, а также на предотвращение несанкционированного доступа, их изменения или распространения таких данных.

Любому лицу должна быть предоставлена возможность: знать о существовании автоматизированного файла персональных данных; знать его основные цели, а также название и местонахождение контролера файла; получить через разумный промежуток времени персональные данные в доступной для понимания форме; добиваться в случае необходимости исправления или уничтожения таких данных, если они подвергались обработке

в нарушение норм внутреннего законодательства; прибегать к средствам правовой защиты в случае невыполнения просьбы о подтверждении или в случае необходимости предоставлении данных, их изменении или уничтожении.

Таким образом, можно сделать следующие выводы:

- любая обработка должна иметь свою цель;
- цель должна быть законной, заранее определенной (отражена в согласии субъекта персональных данных и соответствовать деятельности по их обработке) и конкретной (четко сформулирована);
- для обеспечения целевого характера обработки персональных данных необходимо:
    - иметь раздельные базы данных работников и обучающихся, соискателей на рабочее место и абитуриентов;
    - обеспечивать точность и достаточность, а при необходимости и актуальность данных;
    - уничтожать либо обезличивать данные, если цели обработки достигнуты или утрачена необходимость в их достижении (не следует хранить персональные данные дольше, чем это необходимо в целях бухгалтерского и налогового учета).

Аналогичные подходы к обработке персональных данных нашли отражение в принципах обработки, изложенных в статье 5 *Федерального закона № 152-ФЗ «О персональных данных»* (далее – Закон № 152-ФЗ), где также говориться о справедливой, законной и целевой обработке, хранении данных. Исчерпывающие случаи такой *обработки без согласия субъекта* персональных данных и условия такой обработки прописаны в статье 6 Закона № 152-ФЗ.

Оператор по обработке персональных данных согласно статьям 18.1, 19, 22.1 Закона № 152-ФЗ *обязан:*

- получать согласие на обработку данных у субъекта персональных данных при передаче такой обработки третьему лицу, предварительно уведомлять уполномоченный орган (Роскомнадзор);
- издавать локальные акты по обработке персональных данных;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним;
- назначать лицо, ответственное за организацию обработки персональных данных;
- проводить работу по обезличиванию персональных данных.

Порядок получения согласия на обработку персональных данных определяется приказом Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения». Согласно статье 22 Закона №152-ФЗ если оператор осуществляет деятельность по

обработке персональных данных исключительно без использования средств автоматизации, то уведомлять Роскомнадзор не нужно.

Методические рекомендации по уведомлению уполномоченного органа о начале обработке персональных данных и о внесении изменений в ранее представленные сведения утверждены приказом Роскомнадзора от 30.05.2017 № 94. При направлении уведомлений следует руководствоваться Порядком, утвержденным Приказом Роскомнадзора от 14.11.2022 № 187.

Требования и методы по обезличиванию персональных данных установлены приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» и соответствующими методическими рекомендациями по применению данного приказа Роскомнадзора, а также письмом Роскомнадзора от 06.09.2022 № 08-80975 «О рассмотрении письма».

Уничтожение персональных данных производится в порядке, предусмотренном приказом Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных» (далее – приказ № 179).

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установлены постановлением Правительства РФ от 15.09.2008 № 687. Осуществление такой обработки осуществляется на основании правовых актов образовательной организации, изданных с учетом данного постановления правительства РФ и нормативных правовых актов отраслевого федерального и регионального органов. Следует отметить, что при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

По смыслу правовых понятий, изложенных выше, *персональные данные это* определенный вид информации, обладающей уточняющими признаками и относящийся только к человеку (персоне), поэтому субъектом персональных данных может быть только человек. Данные юридических лиц персональными данными не являются.

Виды и способы обработки персональных данных

Как уже отмечалось выше, обработка персональных данных представляет собой набор определенных действий, совершаемых с персональными данными. Такие действия и образуют следующие *виды обработки персональных данных*:

- сбор;
- запись;
- систематизация;

- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение;
- распространение;
- предоставление.

Персональные данные обрабатываются *двумя способами*:

1) с использованием средств автоматизации;
2) без использования средств автоматизации.

Персональные данные в зависимости от правового режима их обработки *подразделяются на следующие виды*:

- *Обычные персональные данные* (паспортные данные, ФИО, контактные данные и т.п.);
- *Специальные персональные данные* (биометрические, обезличенные, а также персональные данные, разрешенные субъектом персональных данных для распространения);
- *Обезличенные персональные данные.*

К специальным категориям персональных данных относятся сведения о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, а также сведения о судимости (имеют наиболее жесткие ограничения обработки).

Биометрические сведения – сведения, которые использует оператор персональных данных для установления личности субъекта персональных данных, характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (фотоизображение лица, глаз, опечатки пальцев рук). Обработка биометрических данных требует специального согласия субъекта персональных данных и соблюдения повышенных требований к их защите.

Персональные данные, разрешенные для распространения (которые субъект персональных данных по своей воле размещает в общедоступных источниках).

Обезличенные персональные данные. Действующее законодательство рассматривает обезличенные данные как персональные данные, поскольку их можно деобезличить (сделать снова персональными) данная позиция нашла свое отражение в приказе Роскомнадзора от 05.09.2013 № 996.

Имеющаяся судебная практика свидетельствует, что запись с видеокамеры в коридоре образовательной организации не является биометрическими сведениями, а запись с видеокамеры, предназначенной для контроля управления доступом, может относиться к таким сведениям, т.к. видео изображение человека используется оператором персональных данных для установления его личности.

Обработка персональных данных третьим лицом

Практика обработки персональных данных *допускает их обработку третьими лицами*, но при соблюдении определенных условий.

В статье 6 Закона № 152-ФЗ изложены условия такой обработки, к которым относятся:

- основанием является получение *согласия субъекта персональных данные* на такую обработку, наличие у оператора персональных данных *договора, заключенного с третьим лицом*, наличие *решения государственного или муниципального органа* в виде соответствующего акта;
- лицо, осуществляющее обработку персональных данных по поручению оператора, обязано *соблюдать принципы и правила обработки, соблюдать конфиденциальность, принимать необходимые меры*, направленные на обеспечение выполнения обязанностей, предусмотренных законом о персональных данных;
- лицо, осуществляющее обработку персональных данных *по поручению оператора, не обязано получать согласие субъекта персональных данных* на обработку его данных;
- *ответственность перед субъектом персональных данных за действия указанного лица несет оператор.* Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

Обязанности оператора при получении персональных данных

Оператор обязан предоставить информацию *гражданину, если он об этом просит*, сведения, перечисленные в части 7 статьи 14 Закона № 152-ФЗ, а именно:

- подтвердить факт обработки персональных данных;
- сообщить, цели, сроки передачи персональных данных;
- разъяснить последствия отказа, предоставить данные, если их предоставление является обязательным в соответствии с

федеральным законодательством. Факт такого разъяснения рекомендуется оформить документально, под расписку.

При получении персональных данных оператор обязан:

- дать возможность гражданину определить перечень персональных данных, разрешенных для распространения;
- установить порядок хранения и использования персональных данных;
- ознакомить каждого работника под подпись с Политикой образовательной организации по обработке персональных данных;
- установить перечень лиц, которые имеют доступ к персональным данным.

Общедоступная информация

В работе с персональными данными оператору важно знать, какая *информация является общедоступной*.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон № 149-ФЗ) к таковой информации относятся *общеизвестные сведения и иная информация, доступ к которой не ограничен*.

Общедоступная информация размещается ее обладателями в форме открытых данных в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования. Например, общедоступными сведениями считаются данные реестров операторов, которые ведет Роскомнадзор, данные, полученные из общедоступных источников, таких как социальные сети, интернет-площадки и сервисы, где обладатель разместил или дал согласие на размещение сведений о себе.

Общедоступная информация *может использоваться любыми лицами* по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Права обладателя информации

Согласно статье 6 Закона № 149-ФЗ *обладатель информации*, если иное не предусмотрено федеральными законами, *вправе*:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;

- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обработка персональных данных без средств автоматизации

Особенности обработки таких данных урегулированы постановлением Правительства от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и должны соблюдаться оператором.

Лица, осуществляющие обработку персональных данных без средств автоматизации, должны быть проинформированы об этом и особенностях такой обработки.

В отношении каждой категории обрабатываемых персональных данных должны быть определены места хранения и перечень лиц, имеющих к ним доступ. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных, исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

Глава 3.
ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА О ПЕРСОНАЛЬНЫХ ДАННЫХ

За нарушение законодательства о персональных данных применяются следующие виды ответственности:

1. ***Административная*** за нарушения в работе с персональными данными при несоблюдении требований, установленных:
   - *Трудовым кодексом РФ.* Так в соответствие со статьей 90 ТК РФ лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном настоящим ТК и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами. Например, работодателя могут привлечь к ответственности по части 1, 2 статьи 5.27 КоАП РФ, если он не знакомит работников под подпись с локальными нормативными актами, которые устанавливают порядок обработки персональных данных работников (например, с положением о персональных данных), нарушает правила обработки персональных данных, не выполняет требования по защите персональных данных, не исполняет обязанности по взаимодействию с Роскомнадзором. Также в соответствии с Трудовым кодексом РФ к работнику, нарушающему определенные ему трудовые обязанности по обработке персональных данных, можно применять *дисциплинарную ответственность* в виде замечания, выговора и увольнения.
   - *Законом № 152 «О персональных данных».* Согласно п. 9 ч. 3 ст. 23 данного закона, уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) вправе привлекать к административной ответственности лиц, виновных в нарушении законодательства о персональных данных. Например, при нарушении правил обработки персональных данных.
   - *Кодексом об административных правонарушениях РФ*. Так согласно статье 13.11. КоАП РФ обработка персональных данных в случаях, не предусмотренных законодательством РФ, либо обработка персональных данных, несовместимая с целями сбора персональных данных влечет наложение административного штрафа на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц – от десяти тысяч до двадцати тысяч рублей;

на юридических лиц – от шестидесяти тысяч до ста тысяч рублей. Повторное совершение данного административного правонарушения влечет наложение административного штрафа на граждан в размере от четырех тысяч до двенадцати тысяч рублей; на должностных лиц – от двадцати тысяч до пятидесяти тысяч рублей; на индивидуальных предпринимателей – от пятидесяти тысяч до ста тысяч рублей; на юридических лиц – от ста тысяч до трехсот тысяч рублей.

Обработка персональных данных без согласия в письменной форме субъекта персональных данных на обработку его персональных данных в случаях, когда такое согласие должно быть получено либо обработка персональных данных с нарушением установленных законодательством Российской Федерации в области персональных данных требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных влечет наложение административного штрафа на граждан в размере от шести тысяч до десяти тысяч рублей; на должностных лиц – от двадцати тысяч до сорока тысяч рублей; на юридических лиц – от тридцати тысяч до ста пятидесяти тысяч рублей.

Повторное совершение данного административного правонарушения – влечет наложение административного штрафа на граждан в размере от десяти тысяч до двадцати тысяч рублей; на должностных лиц – от сорока тысяч до ста тысяч рублей; на индивидуальных предпринимателей – от ста тысяч до трехсот тысяч рублей; на юридических лиц – от трехсот тысяч до пятисот тысяч рублей.

Невыполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, определяющему политику оператора в отношении обработки персональных данных, или сведениям о реализуемых требованиях к защите персональных данных – влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до трех тысяч рублей; на должностных лиц – от шести тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей – от десяти тысяч до двадцати тысяч рублей; на юридических лиц – от тридцати тысяч до шестидесяти тысяч рублей.

Невыполнение оператором предусмотренной законодательством РФ в области персональных данных обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, – влечет наложение административного штрафа на граждан в размере от двух тысяч до четырех тысяч рублей; на должностных лиц – от восьми тысяч до двенадцати тысяч рублей; на индивидуальных предпринимателей – от двадцати тысяч до тридцати тысяч рублей; на юридических лиц – от сорока тысяч до восьмидесяти тысяч рублей.

Невыполнение оператором в сроки, установленные законодательством РФ в области персональных данных, требования субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных об уточнении персональных данных, их блокировании или уничтожении в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, – влечет наложение административного штрафа на граждан в размере от двух тысяч до четырех тысяч рублей; на должностных лиц – от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей – от двадцати тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до девяноста тысяч рублей.

Повторное совершение данного административного правонарушения – влечет наложение административного штрафа на граждан в размере от двадцати тысяч до тридцати тысяч рублей; на должностных лиц – от тридцати тысяч до пятидесяти тысяч рублей; на индивидуальных предпринимателей – от пятидесяти тысяч до ста тысяч рублей; на юридических лиц – от трехсот тысяч до пятисот тысяч рублей.

Невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния – влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до четырех тысяч рублей; на должностных лиц – от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей – от двадцати тысяч до сорока тысяч рублей; на юридических лиц – от пятидесяти тысяч до ста тысяч рублей.

Невыполнение оператором, являющимся государственным или муниципальным органом, предусмотренной законодательством Российской Федерации в области персональных данных обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов по обезличиванию персональных данных – влечет наложение административного штрафа на должностных лиц в размере от шести тысяч до двенадцати тысяч рублей.

Невыполнение оператором при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», предусмотренной законодательством Российской Федерации в области

персональных данных, обязанности по обеспечению записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, – влечет наложение административного штрафа на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей; на должностных лиц – от ста тысяч до двухсот тысяч рублей; на юридических лиц – от одного миллиона до шести миллионов рублей.

Повторное совершение данного административного правонарушения – влечет наложение административного штрафа на граждан в размере от пятидесяти тысяч до ста тысяч рублей; на должностных лиц – от пятисот тысяч до восьмисот тысяч рублей; на юридических лиц – от шести миллионов до восемнадцати миллионов рублей.

В силу статьи 13.14 КоАП разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных законодательством – влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц – от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц – от ста тысяч до двухсот тысяч рублей.

2. ***Гражданско-правовая ответственность*** применяется в случае причинения убытков или морального вреда гражданину. Размер компенсации устанавливает суд, если будет доказано наступление вреда.
3. ***Материальная ответственность*** работодателя наступает перед работником, если он своими действиями причинил работнику моральный вред (нравственные и физические страдания) при распространении информации о частной, семейной жизни работника, определяемый в судебном порядке. Материальная ответственность работника перед работодателем может наступить, если работник своими действиями нанес имущественный ущерб работодателю, что подтверждается результатами служебного расследования и актом о причинении ущерба. При этом с работником был заключен договор о соответствующей материальной ответственности, а также работником подписано обязательство о неразглашении сведений, составляющих служебную, коммерческую и иную конфиденциальную информацию. В данном случае при наложении *материальной и дисциплинарной ответственности на работника* с него должно быть затребовано письменное объяснение, создана комиссия по определению ущерба и причин нарушений, составлен акт, а также издан приказ руководителя образовательной организации.

4. ***Уголовная ответственность*** наступает**,** если действия физического лица имеют признаки состава преступления, предусмотренного статьями 137; 140; 272 УК РФ.

Так согласно статье 137 УК РФ незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

Те же деяния, совершенные лицом с использованием своего служебного положения, – наказываются штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет, либо принудительными работами на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового, либо арестом на срок до шести месяцев, либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет.

Незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия, – наказывается штрафом в размере от ста пятидесяти тысяч до трехсот пятидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от восемнадцати месяцев до трех лет, либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет или без такового, либо арестом на срок до шести месяцев, либо

лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до шести лет.

В соответствие со статьей 140 УК РФ неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации, если эти деяния причинили вред правам и законным интересам граждан, – наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо лишением права занимать определенные должности или заниматься определенной деятельностью на срок от двух до пяти лет.

В силу статьи 272 УК РФ неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, – наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

То же деяние, причинившее крупный ущерб (сумма которого превышает один миллион рублей) или совершенное из корыстной заинтересованности, – наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

Вышеперечисленные деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, – наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

Вышеперечисленные деяния, если они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет.

ГЛАВА 4.
ФУНКЦИИ И ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАБОТКЕ, ПОЛУЧЕНИИ И ХРАНЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Напомним, что при обработке персональных данных оператор определяет цели обработки, состав обрабатываемых данных и операции, совершаемые с персональными данными. Цели, состав и операции с персональными данными определяются самой организацией, в которой действует оператор, исходя из целей создания организации, изложенных в ее учредительных документах, спецификой бизнес-процессов (образовательной деятельности), функционирующих в организации.

Образовательная организация имеет свою специфику, обусловленную ведением образовательного процесса, выполнением социальнозначимых функций и услуг для граждан по заданию учредителя, обработкой персональных данных не только основных работников, несовершеннолетних обучающихся и их родителей (законных представителей), но и педагогов совместителей, привлекаемых из других организаций, а также соискателей трудовых и учебных вакансий. Соответственно перечисленные категории граждан, имеют свои специфические цели, сроки и операции по обработке персональных данных.

За последние годы в системе образования все шире внедряется цифровая образовательная среда, применяются электронные образовательные ресурсы и разнообразные информационные технологии, активно используются различные государственные информационные системы и сервисы, применяемые в оценке образовательных результатов обучающихся (электронные журналы и дневники). Все это, наряду с исполнением основных обязанностей оператора персональных данных, накладывает определенный отпечаток на специфику обработки персональных данных в образовательной организации.

Основные обязанности оператора персональных данных прописаны в статьях 18 и 18.1 Закона № 152-ФЗ.

Согласно статье 18 Закона № 152-ФЗ *оператор при сборе персональных данных обязан предоставить субъекту персональных данных* по его просьбе информацию, касающуюся обработки его персональных данных, в том числе содержащую:

1) подтверждение факта обработки персональных данных оператором;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые оператором способы обработки персональных данных;
4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным

данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 Закона № 152-ФЗ;

11) иные сведения, предусмотренные федеральными законами.

В соответствии со статьей 18.1 Закона № 152-ФЗ оператор обязан не только принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных нормативными правовыми актами, изданными во исполнение указанного закона, но и самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, касающихся:

1) назначения оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;

2) издания оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений. Такие документы и локальные акты не могут содержать положения, ограничивающие права субъектов персональных данных, а также возлагающие на операторов не предусмотренные законодательством Российской Федерации полномочия и обязанности;

3) применения правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Закона № 152-ФЗ;

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

5) оценки вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения Закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения своих законных обязанностей;

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

Оператор *обязан опубликовать* или иным образом обеспечить неограниченный доступ к документу, определяющему его *политику в отношении обработки персональных данных*, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, *в том числе на страницах принадлежащего оператору сайта* в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

По запросу уполномоченного органа по защите прав субъектов персональных данных (*Роскомнадзора*) оператор обязан *представить документы и локальные акты*, подтверждающие принятие вышеуказанных мер и обязанностей.

§ 4.1.
ФУНКЦИИ И ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ

Общие требования при обработке персональных данных работников

Согласно статьям 86-88 ТК РФ обработка персональных данных работников осуществляется только в целях обеспечения соблюдения законов и нормативных правовых актов. Например, для содействия в трудоустройстве, получении образования, продвижения по службе, для соблюдения личной безопасности работников, контроля количества и качества работы, сохранности имущества.

Работодатель при обработке, хранении персональных данных руководствуется Конституцией РФ, Законом № 152-ФЗ, ТК РФ и должен сообщить работнику о целях, источниках и способах обработки персональных данных. При этом все персональные данные следует получать у самого работника, передача третьим лицам без письменного согласия работника и ознакомления с локальным актом не допускается.

Работодатель не вправе обрабатывать специальные персональные данные (о здоровье, частной жизни и общественной деятельности), кроме случаев, предусмотренных ТК РФ Законом № 152-ФЗ и принимать решения, основываясь на них.

Защита персональных данных обеспечивается за счет средств работодателя. Также работодатель обязан знакомить под роспись работников и их представителей с порядком обработки персональных данных, об их правах и обязанностях в этой области.

Работник не вправе отказываться от своих прав на сохранение и защиту тайны.

Работодатель, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Права работников по защите своих персональных данных

Права работников на защиту своих персональных данных изложены в статье 89 ТК РФ и включают:

- предоставление работникам полной информации об их персональных данных и обработке этих данных;
- свободный бесплатный доступ работникам к своим персональным данным, включая право на получение копий любой записи, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;

- доступ работников к медицинской документации, отражающей состояние их здоровья;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Обработка персональных данных лиц,
не являющихся работниками образовательной организации

Работодателю до начала обработки персональных данных следует уведомить Роскомнадзор о намерении это делать, получить согласие на обработку персональных данных у кандидатов на принимаемую должность (рабочее место), которые необходимы для составления анкеты. Это можно сделать по электронной почте с подтверждением согласия кандидата.

Если необходимость в обработке персональных данных кандидатов отпала, то *персональные данные уничтожаются в течение 30 дней.*

Согласие на обработку *персональных данных, разрешенных субъектом персональных данных для распространения, оформляют отдельно* от иных его согласий на обработку персональных данных.

Способы получения согласия на обработку персональных данных

Согласие на обработку персональных данных оператор получает в случаях, установленных законодательством или в иных случаях по усмотрению оператора персональных данных (при передаче персональных данных третьим лицам, в коммерческих интересах работодателя).

Согласие можно получить в письменной форме (если данная форма предусмотрена законом). Согласие подписывается собственноручно субъектом персональных данных, возможно подписание усиленной квалифицированной электронной подписью или простой электронной подписью субъекта персональных данных в зависимости от целей обработки и состава персональных данных. Согласие должно соответствовать требованиям, установленным приказом Роскомнадзора от 24.02.2021 № 18.

Согласие можно получить в любой форме, позволяющей подтвердить факт того, что согласие действительно получено (Например, расписка членов семьи работника на обработку их персональных данных при оформлении путевки в детский лагерь, гриф «согласен на обработку данных» в анкете).

Согласие должно быть конкретным, информированным и сознательным, позволяющим однозначно сделать вывод о целях, способах обработки персональных данных с указанием действий, совершаемых с персональными данными, объеме обрабатываемых персональных данных. *Одно согласие соответствует одной цели обработки*. Срок согласия отражается в его форме или может быть установлен датой или определенным событием, которое точно наступит.

Случаи, когда согласия субъекта персональных данных на обработку персональных данных, не нужно

Согласие на обработку персональных данных не требуется:

- для заключения договора по инициативе гражданина или договора, по которому он будет выгодоприобретателем или поручителем;
- исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является гражданин;
- *осуществления и выполнения функций, полномочий и обязанностей, которые возложены на образовательную организацию действующим законодательством*;
- осуществления прав и законных интересов субъекта персональных данных или третьих лиц либо *для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы гражданина* (например, если работник на посту охраны записывает Ф.И.О. и паспортные данные посетителей в целях обеспечения безопасности и соблюдения правил пропускного режима).

В остальных случаях обработка персональных данных осуществляется с согласия гражданина в соответствии с пунктом 1 части 1 статьи 6 Закона № 152-ФЗ. Например, придется получить согласие, если работодатель собирает данные граждан для маркетингового, социологического исследования или для оформления пропуска в образовательную организацию (биометрические данные).

Хранение персональных данных уволенных работников

При увольнении работника необходимо проверить, какие сведения о нем имеются у организации, уничтожить те сведения, которые более не нужны.

Должны остаться только те сведения, которые нужны для соблюдения требований законодательства. Например, для ведения кадрового и налогового учета и соблюдения сроков хранения архивных документов.

Бумажное личное дело работника архивируется по установленным правилам и после этого положения Закона № 152-ФЗ к нему не применяется.

Обработка и передача третьим лицам персональных данных работников

Работодатель должен обрабатывать персональных данных исключительно в целях, перечисленных в статье 86 ТК РФ (для обеспечения соблюдения законов и иных НПА, содействия работникам в трудоустройстве, получения образования и продвижения по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества), а также в коммерческих целях при наличии письменного согласия работника.

Передача персональных данных третьим лицам должна осуществляться в случаях, когда это прямо предусмотрено законом (передача сведений в банк и страховую компанию, сервису, оказывающему услуги работникам образовательной организации) и *при условии наличия письменного согласия* работника.

§ 4.2. ФУНКЦИИ И ОБЯЗАННОСТИ ОПЕРАТОРА ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ

Часть 1 ст. 16 Закона № 273-ФЗ «Об образовании в РФ» (далее – Закон № 273-ФЗ) предусматривает, что образовательный процесс может строиться посредством электронного обучения (далее – ЭО) с использованием, в том числе информационно-телекоммуникационных сетей, обеспечивающих взаимодействие обучающихся и педагогов. Федеральные образовательные стандарты общего и среднего профессионального образования предусматривают применение в образовательной деятельности электронного обучения, дистанционных образовательных технологий. Использование электронной информационно-образовательной среды с применением различных электронных образовательных платформ в образовательном процессе невозможно осуществлять без обработки персональных данных обучающихся.

При организации образовательного процесса образовательная организация обязана фиксировать его ход, отражать результаты освоения образовательной программы, фиксировать результаты промежуточной аттестации, доводить данную информацию до обучающихся и их родителей (законных представителей), использовать эти данные для решения задач управления образовательной деятельностью. Данные задачи достигаются путем ведения журнала успеваемости в электронном виде и дневника обучающегося в электронном виде. При этом имеет место быть обработка персональных данных обучающихся с применением электронных сервисов. Такая работа требует определенной регламентации и локального регулирования. Также следует

учесть то, что обработка персональных данных в образовательной организации осуществляется в зависимости от того, какие информационные системы, какие электронные сервисы и платформы используются для такой обработки и какой класс присвоен этим информационным системам по результатам аттестационных (сертификационных) испытаний. В целях оказания методической помощи в работе с информационными системами необходимо использовать письмо Рособразования от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных» и письмо Минобрнауки России от 15.02.2012 № АП-147/07, в которых изложены указания по работе с персональными данными и представлены методические рекомендации по внедрению систем ведения электронных журналов успеваемости в школе.

Обработка персональных данных лиц, поступающих на обучение (абитуриентов) в образовательную организацию, осуществляется аналогично тем условиям, при которых осуществляется обработка персональных данных лиц, не являющихся работниками образовательной организации.

Чтобы не допустить нарушений в работе с персональными данными в ряд статей Закона 273-ФЗ внесены определенные требования, согласно которым обработка персональных данных обучающихся осуществляется *в федеральных информационных системах, федеральных базах данных в сфере образования*, которые формирует и ведет уполномоченный федеральный орган исполнительной власти в сфере образования.

В силу части 3 статьи 16 Закона № 273-ФЗ при реализации основных общеобразовательных программ и образовательных программ среднего профессионального образования с применением электронного обучения, дистанционных образовательных технологий, предусматривающих обработку персональных данных обучающихся, организация, осуществляющая образовательную деятельность должна использовать *государственные информационные системы*, создаваемые, модернизируемые и эксплуатируемые для реализации указанных образовательных программ.

В целях информационного обеспечения управления в системе образования и государственной регламентации образовательной деятельности уполномоченными органами государственной власти и органами государственной власти субъектов РФ создаются, формируются и ведутся государственные информационные системы (далее – ГИС), в том числе ГИС, предусмотренные Законом № 273-ФЗ.

Ведение ГИС осуществляется в соответствии с едиными организационными, методологическими и программно-техническими принципами, обеспечивающими совместимость и взаимодействие этих информационных систем с иными ГИС и информационно-телекоммуникационными сетями, включая информационно-технологическую и коммуникационную инфраструктуры, используемые для предоставления государственных и муниципальных услуг с обеспечением конфиденциальности

и безопасности содержащихся в персональных данных и с соблюдением требований законодательства РФ о государственной тайне.

Кроме того, обработка персональных данных обучающихся осуществляется в целях обеспечения предоставления государственными (муниципальными) образовательными учреждениями услуг, предоставляемых в электронной форме. Перечень таких услуг в сфере образования утвержден распоряжением Правительства от 25.04.2011 № 729-р.

В нем речь идет о следующих услугах:

- по зачислению детей в детские сады и постановки их на соответствующий учет (электронная очередь);
- по предоставлению гражданам информации о реализации на территории региона (муниципального образования) программ дошкольного, общего образования и дополнительных общеобразовательных программ;
- о реализации программ начального и среднего профессионального образования, а также дополнительных профессиональных образовательных программ;
- о результатах сданных экзаменов, результатах тестирования и иных вступительных испытаний, а также о зачислении в государственное образовательное учреждение региона, информации о текущей успеваемости учащегося в государственном (муниципальном) образовательном учреждении региона, о ведении дневника и журнала успеваемости, информации об образовательных программах и учебных планах, рабочих программах учебных курсов, предметах, дисциплинах (модулях), годовых календарных учебных графиках, информации о порядке проведения государственной (итоговой) аттестации обучающихся, освоивших основные и дополнительные общеобразовательные (за исключением дошкольных) и профессиональные образовательные программы, информации из базы данных региона о результатах единого государственного экзамена;
- предоставление информации о результатах сданных экзаменов, результатах тестирования и иных вступительных испытаний, а также о зачислении в муниципальное образовательное учреждение;
- предоставление информации из федеральной базы данных о результатах единого государственного экзамена.

Для государственной итоговой аттестации (далее – ГИА) обучающихся, освоивших программы основного общего образования, среднего общего образования и приема в образовательные организации среднего профессионального образования (далее – СПО) создаются: федеральная система проведения ГИА и федеральная информационная система приема в учреждения СПО, а также региональная информационная система проведения

итоговой аттестации основного общего и среднего общего образования (далее – РИС ИА).

Организация формирования и ведения ФИС и РИС ИА осуществляется соответственно Рособрнадзором и министерствами образования регионов, которые соответственно устанавливают требования по работе в них с персональными данными с учетом Порядка формирования и ведения федеральных информационных систем, утвержденного постановлением Правительства РФ от 10.04.2023 г. № 577.

В целях обеспечения единства требований к осуществлению государственного надзора в сфере образования и учета его результатов Рособрнадзором формируется и ведется ГИС государственного надзора в сфере образования. Порядок формирования данной ГИС установлен Законом № 273-ФЗ (статья 98) и постановлением Правительства РФ от 20.08.2013 г. № 719.

Для ведения реестра документов об образовании, выдаваемых образовательными организациями используется ФИС «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» (далее – ФИС ФРДО). Перечень сведений, вносимых в ФИС ФРДО, порядок ее формирования и ведения, порядок и сроки внесения в нее сведений установлены постановлением Правительства от 31.05.2021 г. № 825.

Все вышеперечисленные случаи обработки персональных данных обучающихся должны осуществляться с учетом совокупного соблюдения требований федерального законодательства в области образования и законодательства по защите персональных данных.

Меры, принимаемые оператором из числа государственных (муниципальных) органов при обработке персональных данных

В случаях, когда обработка персональных данных обучающихся осуществляется оператором из числа государственных (муниципальных) органов, на таких операторов возлагаются дополнительные обязанности, предусмотренные постановлением Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

К таким дополнительным мерам относятся:

- ✓ назначение ответственного служащего за такую работу с заключением с ним соответствующего трудового договора;
- ✓ принятие правовых, организационных и технических мер по обеспечению безопасности персональных данных при эксплуатации информационных систем персональных данных;

- ✓ организация проведения периодических проверок условий обработки персональных данных;
- ✓ ознакомление служащих, осуществляющих обработку персональных данных с законодательством и локальными актами;
- ✓ уведомление Роскомнадзора;
- ✓ обезличивание персональных данных в соответствии с приказом Роскомнадзора от 05.09.2013 № 996;
- ✓ утверждение актом руководителя государственного (муниципального) органа *следующих документов*:
- Правил обработки персональных данных;
- Правил рассмотрения запросов субъектов персональных данных;
- Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- Перечня должностей служащих органа, замещение которых предусматривает осуществление обработки персональных данных либо доступ к ним;
- Должностного регламента ответственного за организацию обработки персональных данных;
- Типового обязательства служащего, осуществляющего обработку, прекратить ее после расторжения служебного контракта (трудового договора);
- Порядка доступа служащих в помещения, где ведется обработка персональных данных.

При разработке вышеперечисленных документов в качестве примерного образца можно использовать документы, утвержденные приказом Минпросвещения России от 14.02.2022 № 74 «Об обработке и обеспечении защиты персональных данных в Министерстве просвещения Российской Федерации».

Глава 5.
МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ЛОКАЛЬНОМ УРОВНЕ

Необходимость защиты персональных данных

Бизнес-процесс, в нашем случае, образовательный процесс и хозяйственная операция либо жизнеобеспечительная деятельность любого субъекта экономической деятельности связаны, так или иначе, с обработкой персональных данных работников, клиентов, партнеров, потребителей. Деятельность образовательной организации в данном случае не является исключением. Образовательная организация первоначально обрабатывает персональные данные детей, желающих поступить на обучение, педагогических и иных работников, желающих устроиться на работу, а затем обрабатывает персональные данные своих сотрудников и обучающихся.

Основная обязанность оператора персональных данных состоит в том, чтобы построить систему управления в коллективе сотрудников и обучающихся таким образом, чтобы Закон № 152-ФЗ соблюдался, начиная с поста охраны при входе в учебное заведение и заканчивая отделом кадров, бухгалтерией, учебной частью и всеми другими подразделениями образовательной организации. Таким образом, у руководителя учреждения стоит сложная комплексная задача по защите персональных данных, которую следует решать системно с применением правовых, организационных и технических мер.

Выше мы сообщали, что в соответствии со статьями 18.1. и 19 Закона № 152-ФЗ оператор персональных данных обязан создать систему организационно-распорядительной и юридической документации и по запросу Роскомнадзора обязан представить документы и локальные акты, подтверждающие принятие мер по защите персональных данных.

Защита персональных данных, осуществляемая оператором

Защита персональных данных, осуществляемая оператором достигается, в частности:

1) *определением угроз безопасности* персональных данных при их обработке в информационных системах персональных данных;

2) *применением организационных и технических мер по обеспечению безопасности* персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) *применением* прошедших в установленном порядке процедуру оценки соответствия *средств защиты информации*;

4) *оценкой эффективности принимаемых мер* по обеспечению безопасности персональных данных *до ввода в эксплуатацию информационной системы* персональных данных;

5) *учетом машинных носителей* персональных данных;

6) *обнаружением фактов несанкционированного доступа* к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

7) *восстановлением персональных данных*, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) *установлением правил доступа к персональным данным*, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) *контролем за принимаемыми мерами* по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

Требования к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных, установлены постановлением Правительства РФ от 01.11.2012 № 1119, требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных утверждены постановлением Правительства РФ от 06.07.2008 № 512. Данными документами и следует руководствоваться в этой работе.

Организационные меры по защите персональных данных

Если образовательная организация выступает оператором по обработке персональных данных, то согласно статье 22.1 Закона № 152-ФЗ она обязана принять меры организационного характера по защите персональных данных, а именно *назначить лицо, ответственное за организацию обработки персональных данных* в образовательной организации.

Данное лицо получает указания непосредственно от руководителя учреждения, и подотчетно ему, кроме того оно, в частности, обязано:

- осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о

персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, 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.

В рамках реализации организационных мер защиты персональных данных оператор проводит работу по *оценке вреда, который может быть причинен субъектам персональных данных* в случае нарушения Закона № 152-ФЗ, определению соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных этим Законом, руководствуясь при этом Требованиями к оценке вреда, который может быть причинен субъектам персональных данных (далее – Требования), утвержденными приказом Роскомнадзора от 27.10.2022 № 178.

Результаты оценки вреда следует оформить актом оценки вреда, который должен содержать:
- наименование или фамилию, имя, отчество (при наличии) и адрес оператора;
- дату издания акта оценки вреда;
- дату проведения оценки вреда;
- фамилию, имя, отчество (при наличии), должность лиц (лица) (при наличии), проводивших оценку вреда, а также их (его) подпись;
- степень вреда, который может быть причинен субъекту персональных данных, в соответствии с Требованиями.

Акт оценки вреда в электронной форме, подписанный электронной подписью, признается электронным документом, равнозначным акту оценки вреда на бумажном носителе, подписанному собственноручной подписью.

Если по итогам проведенной оценки вреда установлены разные степени вреда, применению подлежит более высокая степень вреда.

Правовые меры по защите персональных данных

В качестве *правовых мер защиты персональных данных* образовательная организация – оператор персональных данных – *принимает локальные акты* по вопросам обработки персональных данных, *устанавливает на локальном уровне* перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей

их обработки или при наступлении иных законных оснований, а также *принимает локальные акты, устанавливающих процедуры*, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

Также оператор издает *приказ о назначении лица, ответственного за организацию обработки персональных данных физических лиц* и *приказ об утверждении перечня работников, имеющих доступ к персональным данным физических лиц*, *организует оформление соглашений о конфиденциальности с работниками, имеющими доступ* к персональным данным. В этом соглашении работники, которые сталкиваются с персональными данными ваших работников, обучающихся и их законных представителей, потребителей образовательных услуг, клиентов или партнеров, обязуются не разглашать их.

Оператор *вправе принять отдельный локальный акт об осуществлении внутреннего контроля и (или) аудита* соответствия обработки персональных данных Закону № 152-ФЗ и принятым на его основании нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

Организационные и технические меры защиты персональных данных

Образовательная организация – оператор персональных данных – обязана принимать *организационные и технические меры по обеспечению безопасности персональных данных* при их обработке. Конкретный перечень этих мер зависит от того, в каком виде хранятся данные – в электронном виде или на бумажном носителе.

В отношении данных на бумажных носителях достаточно ограничить и контролировать физический доступ к ним. Например, хранить данные в специальных помещениях либо в специальных шкафах (сейфах) с ограниченным доступом.

Сложнее организовать *защиту электронных данных, обрабатываемых в информационных системах*. Состав организационных и технических мер по защите персональных данных определен постановлением Правительства РФ от 01.11.2012 № 1119, приказом ФСТЭК России от 18.02.2013 № 21, приказом ФСБ России от 10.07.2014 № 378 и зависит от *класса защищенности информационной системы*, используемой при обработке персональных данных. Существуют четыре класса защищенности информационных систем: первый класс (К1); второй класс (К2); третий класс (К3); четвертый класс (К4), определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – четвертый, самый высокий – первый.

Состав и эффективность организационных и технических мер защиты информации в информационной системе зависит от качества *определения угроз безопасности информации для конкретной информационной системы* в

конкретных условиях ее функционирования, *от ее структурно-функциональных характеристик*.

Класс защищенности информационной системы определяется в зависимости от уровня значимости информации, обрабатываемой в этой информационной системе, и масштаба информационной системы (федеральный, региональный, объектовый). В зависимости от класса защищенности информационной системы оператором информационной системы *определяется базовый набор мер защиты информации*.

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации.

Степень возможного ущерба определяется обладателем информации (заказчиком) и (или) оператором самостоятельно экспертным или иными методами и может быть *высокой, средней и низкой*.

Кроме того, для защиты электронных данных образовательная организация должна *взаимодействовать с государственной системой обнаружения, предупреждения и ликвидации последствий кибератак* на информационные ресурсы Российской Федерации (ГосСОПКА), включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных, осуществляется через Национальный координационный центр по компьютерным инцидентам. При таком взаимодействии следует руководствоваться Порядком, утвержденным Приказом ФСБ России от 13.02.2023 № 77.

В рамках реализации организационно-технических мер по защите, используемых информационных систем персональных данных образовательная организация формирует *Модель угроз безопасности информации,* которая представляет собой формализованное описание угроз безопасности информации для конкретной информационной системы или группы информационных систем в определенных условиях их функционирования.

Модель угроз безопасности информации разрабатывается обладателем информации (оператором, разработчиком (проектировщиком)) и должна по содержанию соответствовать Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы, разрабатываемые и утверждаемые ФСТЭК России.

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", *оператор*:

- *обязан* обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с *использованием баз данных, находящихся на территории Российской Федерации*, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Закона №152-ФЗ;
- *обязан осуществлять учет количества экземпляров материальных носителей* и присваивать материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель;
- *вправе установить* не противоречащие требованиям законодательства РФ *дополнительные требования к технологиям хранения биометрических персональных данных* вне информационной системы персональных данных.

Работа по обезличиванию данных

Одной из форм защиты персональных данных оператором является проведение мероприятий по обезличиванию персональных данных. Требования и методы по обезличиванию персональных данных утверждены приказом Роскомнадзора от 05.09.2013 № 996 (далее – приказ № 996), и по применению данного приказа Роскомнадзором разработаны соответствующие методические рекомендации.

К методам по обезличиванию персональных данных, установленным приказом № 996, относятся:

- *метод введения идентификаторов* – замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным;
- *метод изменения состава или семантики* – изменение состава или семантики персональных данных путем замены результатами статистической обработки, преобразования, обобщения или удаления части сведений;
- *метод декомпозиции* – разделение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств;
- *метод перемешивания* – перестановка отдельных значений или групп значений атрибутов персональных данных в массиве персональных данных.

Результаты сопоставления свойства обезличенных данных с методами обезличивания приведены в следующей Таблице.

Соответствие методов обезличивания
свойствам обезличенных данных

Таблица

Метод обезличивания / Свойства обезличенных данных	Метод введения идентификаторов	Метод изменения состава или семантики	Метод декомпозиции	Метод перемешивания
Полнота	+	+/-	+	+
Структурированность	+	+	+	+
Релевантность	+/-	+	+	+
Семантическая целостность	+	+/-	+	+
Применимость	+	+	+	+
Анонимность	+/-	+	+/-	+
+ безусловное наличие свойства +/- условное наличие свойства, см. описание метода				

При использовании оператором процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

Обезличивание персональных данных субъектов должно производиться оператором *перед внесением их в информационную систему*.

Оператор вправе обрабатывать в информационной системе обезличенные данные, полученные от третьих лиц.

В процессе обработки обезличенных данных оператором, при необходимости, *может проводиться деобезличивание*. После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций деобезличивания должна осуществляться в соответствии с действующим законодательством Российской Федерации с применением мер по обеспечению безопасности персональных данных.

Обработка обезличенных данных должна осуществляться с использованием технических и программных средств, соответствующих форме представления и хранения данных.

Обработка персональных данных организаций, не обладающих квалифицированным персоналом либо достаточными материально-техническими средствами, возможна с привлечением сторонних организаций – операторов на основании договора. При использовании технологий «облачной»

обработки персональных данных возможна обработка одним оператором обезличенных данных нескольких подобных организаций.

При обработке обезличенных данных необходимо выделять зоны ответственности операторов, субъектов и/или организаций, поручивших обработку оператору.

Алгоритмы для реализации процедур обезличивания и программное обеспечение должны обеспечивать переносимость на различные аппаратные платформы.

Действия, связанные с внесением изменений и дополнений в массив обезличенных данных, следует проводить в режиме транзакций и отражать в соответствующем журнале.

Следует вести архив запросов на обработку данных.

Субъект персональных данных должен иметь возможность получить сведения о составе его персональных данных, имеющихся у оператора.

Хранение и защиту дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания, следует обеспечить в соответствии с внутренними процедурами обеспечения конфиденциальности, установленными у оператора. При этом должно обеспечиваться исполнение установленных правил доступа пользователей к хранимым данным, *резервного копирования* и возможности актуализации и восстановления хранимых данных.

Процедуры обезличивания/деобезличивания должны встраиваться в процессы обработки персональных данных как их неотъемлемый элемент, а также максимально эффективно использовать имеющуюся у оператора инфраструктуру, обеспечивающую обработку персональных данных.

Оператору рекомендуется разработать и применять при осуществлении своей деятельности *документацию*, включающую:

- ✓ описание применяемых процедур и их программного обеспечения;
- ✓ инструкции по проведению процедур обезличивания/деобезличивания;
- ✓ инструкции по обработке обезличенных данных;
- ✓ инструкции проведения контроля качества обезличенных данных и процедур обезличивания;
- ✓ порядок взаимодействия с другими операторами;
- ✓ инструкции по обеспечению безопасности дополнительной (служебной) информации, содержащей параметры методов и процедур обезличивания/деобезличивания;
- ✓ техническую и эксплуатационную документацию, поставляемую с программными средствами, обезличивания/деобезличивания.

Оператору при обезличивании персональных данных следует:

- ✓ обеспечить соответствие процедур обезличивания/деобезличивания персональных данных требованиям к обезличенным данным и методам обезличивания;

- ✓ обеспечить соответствие процедур обезличивания/деобезличивания условиям и целям обработки персональных данных;
- ✓ убедиться, что при реализации процедур обезличивания/ деобезличивания, а также при последующей обработке обезличенных данных не нарушаются права субъекта персональных данных.

В случае, когда обработка обезличенных данных была поручена оператору третьим лицом, оператору следует соблюдать все требования, предъявляемые этим лицом.

В процессе реализации процедуры обезличивания персональных данных оператору следует соблюдать все регламентные требования, предъявляемые к выбранному способу реализации процедуры обезличивания.

При хранении обезличенных данных оператору следует:

- ✓ организовать *раздельное хранение обезличенных данных* и дополнительной (служебной) информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания;
- ✓ обеспечивать *конфиденциальность* дополнительной (служебной) информации о *выбранном методе* реализации процедуры *обезличивания и параметрах процедуры обезличивания*.

При передаче вместе с обезличенными данными информации о выбранном методе реализации процедуры обезличивания и параметрах процедуры обезличивания *оператору следует обеспечить конфиденциальность канала (способа) передачи данных.*

В ходе реализации процедуры деобезличивания оператору следует:

- ✓ реализовать все требования по обеспечению безопасности получаемых персональных данных при автоматизированной обработке на средствах вычислительной техники, участвующих в реализации процедуры деобезличивания и обработке деобезличенных данных;
- ✓ обеспечить обработку и защиту деобезличенных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Работа по уничтожению персональных данных

Оператор обязан в соответствии с Требованиями к подтверждению уничтожения персональных данных, установленными приказом Роскомнадзора № 179 проводить работу по уничтожению персональных данных субъекта (или обеспечить их уничтожение):

- ✓ *по требованию субъекта* персональных данных (или его представителя), если он установит, что персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не

являются необходимыми для заявленной цели обработки (часть 1 статья 14 Закона № 152-ФЗ);

- ✓ *при предоставлении субъектом* персональных данных или его представителем *сведений, подтверждающих*, что такие персональные данные являются *незаконно полученными или не являются необходимыми* для заявленной цели обработки (часть 3 статья 20 Закона №152-ФЗ);
- ✓ *при выявлении неправомерной обработки* персональных данных, если невозможно обеспечить ее правомерность (часть 3 статья 21 Закона №152-ФЗ);
- ✓ *при достижении цели обработки* персональных данных (часть 4 статья 21 Закона №152-ФЗ);
- ✓ *при отзыве субъектом персональных данных согласия на обработку* его персональных данных, если их сохранение более не требуется для целей обработки персональных данных (часть 5 статья 21 Закона №152-ФЗ).

Согласно приказу № 179, если обработка персональных данных проводится оператором *без использования средств автоматизации*, документом, подтверждающим уничтожение персональных данных, является *акт об уничтожении персональных данных*.

Если обработка персональных данных осуществляется *с использованием средств автоматизации*, документами, подтверждающими уничтожение персональных данных, являются:

- *акт об уничтожении персональных данных;*
- *выгрузка из журнала регистрации событий в информационной системе персональных данных.*

Акт об уничтожении персональных данных в электронной форме, подписанный электронной подписью, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, уничтоживших персональные данные.

Если обработка персональных данных осуществляется оператором *одновременно с использованием средств автоматизации и без их использования*, документами, подтверждающими уничтожение персональных данных, являются *и акт, и выгрузка*.

Акт об уничтожении персональных данных и выгрузку из журнала нужно хранить в течение трех лет с момента уничтожения персональных данных.

Привлечение специалистов по технической защите персональных данных

Следует отметить, что *обеспечение технических мер защиты персональных данных* – это отдельный и серьезный блок работы, который обычно выполняется квалифицированными специалистами в области

информационной безопасности, специализированными организациями, обладающими лицензионными разрешительными документами по технической защите конфиденциальной информации ФСТЭК России и ФСБ России.

Согласно письму Рособразования от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных» для классификации и защиты информационных систем персональных данных образовательные учреждения, не располагающие необходимыми специалистами и лицензиями, могут обратиться на договорных условиях за методической и консультационной поддержкой в организации, имеющие соответствующие лицензии.

Перечень органов (организаций) по аттестации Системы сертификации средств защиты информации по требованиям безопасности информации, а также Государственный реестр сертифицированных средств защиты информации размещены на сайте ФСТЭК России.

Специализированным организациям могут быть поручены:

1. Методическая поддержка и консультирование при проведении сегментирования интегрированных информационных систем, определении состава и классификации информационных систем, обрабатывающих персональные данные;
2. Консультирование и помощь в формировании перечня организационно-технических мероприятий, необходимых для создания системы защиты информационных систем, обрабатывающих персональные данные;
3. Консультирование при подготовке декларации соответствия для систем класса К3;
4. Аудит информационных систем персональных данных, подбор и установка необходимых технических средств защиты информации для систем классов К2 и К1, а также распределенных информационных систем класса К3;
5. Подготовка, проведение аттестационных испытаний информационных систем классов К2 и К1 с выдачей Аттестата соответствия.

При использовании перечисленных нормативно-методических документов по защите персональных данных необходимо иметь в виду, что регулирующими органами могут вноситься уточнения и разъяснения, которые должны приниматься к исполнению всеми операторами информационных систем, обрабатывающих персональные данные.

Глава 6.
ОСОБЕННОСТИ РАЗРАБОТКИ И ПРИНЯТИЯ ЛОКАЛЬНЫХ АКТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ, ЭТАПЫ РАЗРАБОТКИ И СТРУКТУРНЫЕ ЭЛЕМЕНТЫ

Формы и виды локальных актов

Исходя из своего определения локальный нормативный акт (далее – ЛНА) – это правовой распорядительный документ уполномоченного должностного лица организации, сфера применения которого очерчена границами организации, документ, рассчитанный на неоднократное применение и устанавливающий, в частности, права и обязанности (руководителя) работодателя, всех или отдельных работников в части, не урегулированной трудовым и иным законодательством.

ЛНА принимается путем издания приказа (распоряжения) руководителя организации и бывает в виде: Положения, Правил, Инструкции, штатного расписания, графика отпусков и пр.

ЛНА могут быть: *обязательные* (указание на их принятие прямо предусмотрено нормативным правовым актом государственного либо муниципального органа) и *необязательные* (принимаются руководителем по своему усмотрению в целях локального урегулирования бизнес-процессов).

Содержание и структура актов

Структура ЛНА определяется его содержанием и зависит от цели и круга вопросов, в отношении которых необходимо принятие таких актов.

ЛНА должен соответствовать ГОСТ Р 7.0.97-2016 «Организационно-распорядительная документация. Требования к оформлению документов».

Содержание ЛНА должно соответствовать ранее изданным по этому вопросу документам и действующему законодательству.

Для лучшего восприятия текст может быть разделен на отдельные части (разделы, подразделы, пункты и т.д.). Каждой части следует присвоить заголовок, который должен передавать ее краткое содержание.

Условно структуру ЛНА можно разделить на следующие части (разделы):

- ***Общие положения.*** В данном разделе описывается перечень регулируемых вопросов; указываются нормативные правовые акты, в соответствии с которыми ЛНА принимается; уточняется круг вопросов, подразделения или категории работников, подпадающие под действие ЛНА.
- ***Основная часть.*** В данной части прописываются права и обязанности работника и работодателя; устанавливаются процедуры, не определенные

законодательством, порядок взаимодействия структурных подразделений, участников отношений, регулируемых ЛНА в зависимости от специфики организации; описываются действия сторон, сроки, ответственность и пр.

- ***Заключительные положения.*** В разделе указывается время вступления ЛНА в силу, порядок внесения в него изменений и дополнений, а также процедура и случаи его отмены, перечисляется перечень ранее изданных ЛНА или отдельных их положений, которые прекращают свое действие в связи с принятием нового ЛНА.
- ***Приложения***. В данном разделе прикладываются образцы, формы (макеты) примерных, типовых документов, применение которых связано с приятием и исполнением ЛНА.

Порядок разработки и принятия ЛНА

Порядок разработки ЛНА законодательно не установлен, поэтому руководитель образовательной организации определяет его самостоятельно.

Условно *порядок разработки ЛНА можно разделить на следующие стадии:*

- *определение круга вопросов*, по которым следует разработать ЛНА;
- *определение этапов и сроков* разработки ЛНА;
- *создание рабочей группы* по разработке ЛНА;
- *согласование (визирование)* подготовленного проекта ЛНА, в том числе с учетом мнения представительного органа работников в порядке, установленном статьей 372 ТК РФ;
- *утверждение (принятие) и подписание* ЛНА (в приказе по утверждению следует отразить дату введения ЛНА, назначение ответственных за организацию работы и контроль за исполнением ЛНА, а также указать на необходимость ознакомления с ним работников и др.);
- *оформление* ЛНА (проведение регистрации, проставление даты и присвоение номера);
- *обнародование (опубликование)* ЛНА;
- *ознакомление* работников (на листе ознакомления или в специальном журнале, либо на листе ознакомления, прилагаемого к трудовому договору).

Локальные акты о порядке обработки персональных данных в образовательной организации

Конкретный перечень таких документов законодательно не установлен.

Как правило, организации издают *Положение об обработке и защите персональных данных* или иной ЛНА по вопросам их обработки.

В таком документе описывают все связанные с обработкой действия (получение, хранение, использование, передача данных и т.п.).

Для каждой цели обработки указанное Положение должно определять в том числе категории и перечень персональных данных, способы, сроки их обработки и хранения и др. особенности во исполнение статьи 87 ТК РФ, пункта 2 части 1 статьи 18.1 Закона №152-ФЗ.

Кроме Положения об обработке и защите персональных данных в образовательной организации следует разработать и принять *Политику в отношении обработки персональных данных*. Данный документ кратко декларирует принципы, цели и задачи обработки персональных данных, категории обрабатываемой информации и перечисляет применяемые способы такой обработки.

Структуру и содержание Политики организация устанавливает самостоятельно. Для этого можно использовать письмо Роскомнадзора от 19.10.2021 № 08-71063 и соответствующие Методические рекомендации данного уполномоченного органа.

При разработке локальных актов по работе с персональными данными в образовательной организации можно использовать, в качестве примерного образца, прилагаемые к настоящим Методическим рекомендациям формы локальных актов, а также подходы к обработке персональных данных, изложенные в приказе Минпросвещения России от 14.02.2022 № 74 «Об обработке и обеспечении защиты персональных данных в Министерстве просвещения Российской Федерации».

Независимо от способа сбора персональных данных *оператор обязан обеспечить неограниченный доступ к документу, определяющему политику* в отношении обработки персональных данных. Ознакомление работников с Положением и Политикой в отношении обработки персональных данных осуществляется под роспись с учетом норм, установленных пунктом 8 статьи 86, частью 2 статьи 22 ТК РФ.

Политику в отношении обработки персональных данных дополнительно следует опубликовать на сайте образовательной организации во исполнение части 2 статьи 18.1 Закона № 152-ФЗ либо повесить распечатанный бумажный вариант на информационном стенде (см. письмо Роскомнадзора от 19.10.2021 № 08-71063).

Структурные компоненты (разделы) Положения об обработке и защите персональных данных

1. ***Основные понятия*** (персональные данные, конфиденциальная информация, личные данные работников, обучающихся).

2. ***Основные условия проведения обработки персональных данных работников и обучающихся в процессе образовательной деятельности*** (цели, принципы, способы получения персональных данных).
3. ***Хранение и использование персональных данных работников, обучающихся*** (порядок хранения, перечень лиц, имеющих право доступа к ним без предварительного разрешения, порядок копирования персональных данных).
4. ***Передача персональных данных работника, обучающегося*** (требования и запреты при передаче персональных данных, используемые защищенные линии (каналы) связи при передаче персональных данных, обязанности работника и лица передающего персональные данные, случаи, когда согласия субъекта персональных данных на обработку не требуется).
5. ***Права работников, родителей обучающихся в целях обеспечения защиты персональных данных*** (перечень прав работников и законных представителей обучающихся).
6. ***Обязанности работника, родителей обучающегося в целях обеспечения достоверности его персональных данных*** (перечень обязанностей субъектов персональных данных).
7. ***Доступ к персональным данным*** (порядок и случаи доступа, перечень лиц с правом доступа).
8. ***Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников, обучающихся***.
9. ***Заключительные положения*** (срок вступления документа в силу, порядок внесения изменений и дополнений).
10. ***Приложения***:

Приложение № 1. Согласие на обработку персональных данных работника, родителя (законного представителя) обучающегося;
Приложение № 2. Согласие на обработку персональных данных соискателя, абитуриента, родителей (законных представителей) несовершеннолетнего поступающего;
Приложение № 3. Согласие на передачу персональных данных работника, обучающегося, родителей (законных представителей) несовершеннолетнего обучающегося.
Приложение № 4. Обязательство о неразглашении персональных данных.

Структурные компоненты (разделы) Политики
в отношении обработки персональных данных

1. ***Общие положения*** (излагаются основные используемые понятия: обработка персональных данных, оператор, субъект персональных

данных, конфиденциальность персональных данных и т.д.; основные права и обязанности оператора и субъекта(ов) персональных данных).

2. ***Цели сбора персональных данных*** (перечисляется перечень конкретных, заранее определенных и законных целей, обусловленных исполнением нормативных правовых документов, регламентирующих деятельность оператора, учредительных документов оператора и конкретных бизнес-процессов оператора при эксплуатации имеющихся информационных систем и способов обработки).
3. ***Правовые основания обработки персональных данных*** (дается перечень нормативных правовых актов, решений учредителя во исполнение которых и в соответствии с которыми оператор осуществляет обработку персональных данных, перечень договоров, заключенных между оператором и субъектом персональных данных и иных законных оснований на обработку).
4. ***Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных*** (перечисляются категории персонала и контингент обучающихся: работники, обучающиеся, соискатели, абитуриенты, бывшие работники, выпускники, клиенты, контрагенты и объемы данных, подлежащих обработке).
5. ***Порядок и условия обработки персональных данных*** (дается перечень действий, совершаемых оператором с персональными данными субъектов персональных данных, используемые оператором способы обработки персональных данных и сроки обработки персональных данных. В случае необходимости взаимодействия с третьими лицами в рамках достижения целей обработки персональных данных необходимо указывать условия передачи персональных данных в адрес третьих лиц).

ПРИЛОЖЕНИЯ

ОБРАЗЦЫ ОТДЕЛЬНЫХ ЛОКАЛЬНЫХ АКТОВ ПО РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Утверждаю:

_____
(должность руководителя, наименование образовательной организации)

"___"_____ ____ г. № ____

_____/_____
(подпись / Ф.И.О. руководителя)

М.П.

ПОЛОЖЕНИЕ
о защите, хранении, обработке и передаче
персональных данных работников и обучающихся
образовательной организации

1. Общие положения

1.1. Настоящее Положение разработано на основании ст. ст. 86 - 90 Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", Федерального закона от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации".

1.2. В соответствии с п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" под персональными данными работников и обучающихся (далее – персональные данные) понимается любая информация, относящаяся к определенному или определяемому на основании такой информации работнику или обучающемуся, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

1.3. Организация, в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", является оператором, организующим и (или) осуществляющим обработку персональных данных, а также определяющим цели и содержание обработки персональных данных.

1.4. Работники, уполномоченные на обработку персональных данных, обеспечивают обработку персональных данных в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", Федерального закона от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации", Трудового кодекса Российской Федерации, других нормативных правовых актов Российской Федерации и несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты этих персональных данных.

1.5. Перечень лиц, уполномоченных на получение, обработку, хранение, передачу и любое другое использование персональных данных в Организации, утверждается приказом руководителя Организации.

1.6. При получении, обработке, хранении и передаче персональных данных лица, уполномоченные на получение, обработку, хранение, передачу и любое другое использование персональных данных, обязаны соблюдать следующие требования:

а) обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия работникам и обучающимся в прохождении обучения, их карьерном росте, обеспечения личной безопасности и членов их семей, а также в целях обеспечения сохранности принадлежащего им имущества и имущества Организации, учета результатов исполнения ими обязанностей;

б) персональные данные следует получать лично у работников или обучающихся. В случае возникновения необходимости получения персональных данных у третьей стороны следует известить об этом работников и обучающихся заранее, получить их письменное согласие и сообщить работникам и обучающимся о целях, предполагаемых источниках и способах получения персональных данных;

в) запрещается получать, обрабатывать и приобщать к личному делу работников и обучающихся не установленные Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации" и Трудовым кодексом Российской Федерации персональные данные об их политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

г) при принятии решений, затрагивающих интересы работников и обучающихся, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

д) защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств Организации в порядке, установленном Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации", Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации;

е) передача персональных данных третьей стороне не допускается без письменного согласия работников и обучающихся, за исключением случаев, установленных федеральными законами;

ж) работники, обучающиеся и их представители должны быть ознакомлены под подпись с документами Организации, устанавливающими порядок обработки персональных данных, а также с их правами и обязанностями в этой области;
з) работники и обучающиеся не должны отказываться от своих прав на сохранение и защиту тайны;
и) Организация, работники, обучающиеся и их представители должны совместно вырабатывать меры защиты персональных данных.

1.7. Персональные данные, которые обрабатываются в информационных системах, подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.8. Сведения о персональных данных работников относятся к числу конфиденциальных (составляющих охраняемую законом тайну Организации). Режим конфиденциальности в отношении персональных данных снимается:
- в случае их обезличивания;
- по истечении 75 лет срока их хранения;
- в других случаях, предусмотренных федеральными законами.

2. Сохранение персональных данных в образовательной деятельности

2.1. В целях информационного обеспечения управления в системе образования и государственной регламентации образовательной деятельности уполномоченными органами государственной власти Российской Федерации и органами государственной власти субъектов Российской Федерации создаются, формируются и ведутся государственные информационные системы, в том числе государственные информационные системы, предусмотренные Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации". Ведение государственных информационных систем осуществляется в соответствии с едиными организационными, методологическими и программно-техническими принципами, обеспечивающими совместимость и взаимодействие этих информационных систем с иными государственными информационными системами и информационно-телекоммуникационными сетями, включая информационно-технологическую и коммуникационную инфраструктуры, используемые для предоставления государственных и муниципальных услуг, с обеспечением конфиденциальности и безопасности содержащихся в них персональных данных и с соблюдением требований

законодательства Российской Федерации о государственной или иной охраняемой законом тайне.

2.2. Организация гарантирует безопасность и конфиденциальность персональных данных, используемых в целях информационного обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема в образовательные организации для получения среднего профессионального и высшего образования.

2.3. При реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий Организация также обеспечивает защиту персональных данных.

2.4. При поступлении в Организацию обучающиеся представляют достоверные сведения. Организация вправе проверять достоверность представленных сведений.

2.5. Организация обеспечивает взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных.

3. Получение, обработка, хранение персональных данных

3.1. В Организации устанавливается следующий порядок получения персональных данных:

3.1.1. Организация не имеет права получать и обрабатывать персональные данные работника или обучающегося о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни.

3.1.2. В случаях, непосредственно связанных с вопросами трудовых отношений или образования, в соответствии со ст. 24 Конституции Российской Федерации Организация вправе получать и обрабатывать данные о частной жизни работника или обучающегося только с его письменного согласия.

3.2. Обработка персональных данных возможна только с согласия работников и обучающихся либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника или обучающегося, их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов - в случаях, предусмотренных федеральным законом.

3.3. Организация вправе обрабатывать персональные данные работников и обучающихся только с их письменного согласия.

3.4. Письменное согласие работника и обучающегося на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным.

3.5. Цели обработки персональных данных: _____ (каждая организация указывает свои исходя из анализа правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных бизнес-процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных)).

Для достижения указанных целей в Организации обрабатываются следующие персональные данные: _____ (указать категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований).

3.6. Согласие работника или обучающегося не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определенного полномочия Организации;

- обработка персональных данных в целях исполнения трудового договора или договора на обучение;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника или обучающегося, если получение его согласия невозможно.

3.7. Организация обеспечивает безопасное хранение персональных данных, в том числе:

3.7.1. Хранение, комплектование, учет и использование содержащих персональные данные документов организуется в форме обособленного архива Организации. Такой архив ведется в электронном виде и на бумажных носителях.

3.7.2. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.7.3. Хранимые персональные данные подлежат защите от несанкционированного доступа и копирования. Безопасность персональных данных при их хранении обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.7.4. При хранении персональных данных Организация обеспечивает:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных или на

бумажные документы, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

4. Передача персональных данных

4.1. Персональные данные передаются с соблюдением следующих требований:

- запрещается сообщать персональные данные третьей стороне без письменного согласия работника или обучающегося, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или обучающегося, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации";
- не сообщать персональные данные в коммерческих целях без письменного согласия субъекта таких данных;
- предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном Трудовым кодексом Российской Федерации или Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации";
- осуществлять передачу персональных данных в пределах Организации в соответствии с локальным нормативным актом, с которым работник или обучающийся должен быть ознакомлен под подпись;
- разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника или обучающегося, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции или получения образования;
- передавать персональные данные работника представителям работников или обучающегося, представителям обучающихся в

порядке, установленном Трудовым кодексом Российской Федерации или Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных" и Федеральным законом от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации", и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

5. Доступ к персональным данным

5.1. Право доступа к персональным данным имеют:
- руководитель Организации;
- работники отдела кадров;
- работники бухгалтерии;
- начальник отдела экономической безопасности (информация о фактическом месте проживания и контактные телефоны);
- работники секретариата (информация о фактическом месте проживания и контактные телефоны);
- начальник отдела внутреннего контроля (доступ к персональным данным работников в ходе плановых проверок);
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения).

5.2. Права работников и обучающихся в целях обеспечения защиты персональных данных:
- на полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и Федерального закона от 29.12.2012 № 273-ФЗ "Об образовании в Российской Федерации". При отказе Организации исключить или исправить персональные данные работник или обучающийся имеет право заявить в письменной форме Организации о своем несогласии с соответствующим обоснованием такого несогласия. Персональные

данные оценочного характера работник или обучающийся имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении Организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия Организации при обработке и защите его персональных данных.

5.3. Копировать и делать выписки персональных данных разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров.

6. Ответственность за нарушение норм, регулирующих обработку персональных данных

6.1. Лица, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

6.2. Руководитель Организации за нарушение порядка обращения с персональными данными несет административную ответственность в соответствии с Кодексом Российской Федерации об административных правонарушениях, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом работнике.

6.3. Работники Организации, допустившие разглашение персональных данных другого работника или обучающегося, могут быть уволены по инициативе работодателя по пп. «в» ч. 6 ст. 81 Трудового кодекса Российской Федерации. Увольнение не исключает иных форм ответственности, предусмотренной действующим законодательством.

С настоящим Положением ознакомлен(а):

"___"_____ ____ г. _____ _____/_____
(должность, подпись/Ф.И.О.)

"___"_____ ____ г. _____ _____/_____
(должность, подпись/Ф.И.О.)

"___"_____ ____ г. _____ _____/_____
(должность, подпись/Ф.И.О.)

"___"_____ ____ г. _____ _____/_____
(должность, подпись/Ф.И.О.)

_____
(наименование, ОГРН, ИНН, КПП, адрес, телефон, адрес электронной почты организации)

ПРИКАЗ № _____
об утверждении политики обработки персональных данных

г. _____ "___"_____ ____ г.

В связи с необходимостью обработки персональных данных работников, представителей контрагентов (клиентов, абонентов – физических лиц) _____ (наименование организации), руководствуясь ст. 7 Конвенции о защите физических лиц при автоматизированной обработке персональных данных (закл. в г. Страсбурге 28.01.1981), ст. ст. 6, 7 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", гл. 14 Трудового кодекса Российской Федерации, ст. ст. 150 - 152.2 Гражданского кодекса Российской Федерации, ст. 137 Уголовного кодекса Российской Федерации, ст. 13.11 Кодекса Российской Федерации об административных правонарушениях, а также соответствующими им подзаконными и локальными нормативными актами, п. _._ ст. _____ _____ (наименование акта о деятельности юридического лица в части обработки персональных данных), п. ___ Устава _____ "_____" от "___"_____ ____ г., приказываю:

1. Утвердить Политику обработки персональных данных _____ "_____" с "___"_____ 20__ г.
2. Начальнику службы кадров _____ (Ф.И.О.) совместно с начальником юридической службы _____ (Ф.И.О.) и начальником _____ (название структурного подразделения) руководствоваться в своей деятельности утвержденной Политикой обработки персональных данных _____ "_____".
3. Начальнику службы кадров _____ (Ф.И.О.) довести настоящий Приказ до сведения работников _____ "_____".
4. Контроль за исполнением настоящего Приказа возложить на _____ (должность, Ф.И.О. работника) (вариант: оставляю за собой).

Приложение:
Политика обработки персональных данных _____ "_____" от "___"_____ 20__ г. на __ л. в __ экз.
Руководитель: _____/_____
(подпись) (Ф.И.О.)

С Приказом ознакомлены:
"__"_____ ____ г.
_____/_____
(подпись) (Ф.И.О.)

_____
(полное наименование, адрес, ОГРН, ИНН, КПП оператора персональных данных)

Приказ № _____
об утверждении Положения об обработке персональных данных

г. _____ "__"_____ ____ г.

В соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", руководствуясь 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, приказываю:

1. С "_____"_____ ____ г. утвердить и ввести в действие Положение об обработке персональных данных в _____.
(наименование организации)
2. Контроль за исполнением настоящего Приказа возлагаю на _____.
(Ф.И.О., должность сотрудника)

_____ _____/_____
(должность руководителя юридического лица) (подпись) (Ф.И.О.)

М.П.

С Приказом ознакомлен(а):
"__"_____ ____ г. _____/_____
(подпись) (Ф.И.О.)

_____

(наименование бюджетного учреждения, адрес местонахождения, ОГРН, ИНН)

Приказ № ____

"О назначении лица, ответственного
за организацию обработки персональных данных"

г. _____ "___"_____ ____ г.

На основании п. 1 ч. 1 ст. 18.1, ч. 1 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", руководствуясь 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, приказываю:

1. Назначить _____ (должность работника, Ф.И.О.) ответственным за организацию обработки персональных данных.
2. _____ обеспечить принятие (должность работника, Ф.И.О.) организационных и технических мер, применяемых для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, в срок до _____.
3. В связи с новым назначением _____ (должность работника, Ф.И.О.) внести соответствующие изменения в должностную инструкцию _____ (должность работника, Ф.И.О.).
4. Установить ежемесячную доплату _____ (должность работника, Ф.И.О.) в размере _____ (_____) рублей к должностному окладу в связи с исполнением дополнительной обязанности по организации обработки персональных данных.
5. _____ (должность работника, Ф.И.О.) внести соответствующие изменения в Трудовой договор от "___"_____ ____ г. № ___.
6. Начальнику отдела кадров _____ (Ф.И.О.) ознакомить всех заинтересованных лиц с настоящим приказом.

7. Контроль за исполнением настоящего приказа оставляю за собой (вариант: возложить на _____ (должность работника, Ф.И.О.)).

_____/_____/_____
(должность/подпись/Ф.И.О.)

С Приказом ознакомлены:

"___"_____ _____ г. _____ / _____
(подпись) (должность, Ф.И.О. работника)

"___"_____ _____ г. _____ / _____
(подпись) (должность, Ф.И.О. работника)

"___"_____ _____ г. _____ / _____
(подпись) (должность, Ф.И.О. работника)

Обязательство

о неразглашении персональных данных

Я, Иванова Наталья Ивановна (паспорт 00 11 222222, выдан 00.00.2000 ОВД _____города _____), понимаю, что получаю доступ к персональным данным работников СОШ №1 (ОГРН _____, ИНН _____) и осуществляю их обработку в связи с исполнением своих обязанностей.

Подтверждаю, что за исключением случаев, предусмотренных законодательством, не имею права передавать третьим лицам любые персональные данные работников СОШ №1, включая, но не ограничиваясь сведениями:

о паспортных данных;

образовании;

составе семьи;

воинском учете;

заработной плате;

адресе, телефоне;

месте работы или учебы членов семьи;

данных банковских счетов и карт.

Я ознакомлен(а) с Положением о защите персональных данных работников СОШ №1 и предупреждена, что за разглашение персональных данных работника я могу быть привлечен(а) к ответственности, предусмотренной трудовым, гражданским, административным и уголовным законодательством.

Главный бухгалтер Иванова Иванова Н.И.
00.00.2023

_____
(наименование образовательной организации, адрес местонахождения, ОГРН, ИНН)

Приказ № _____
"О создании комиссии для проведения мероприятий
по защите персональных данных"

г. _____ **"___"_____ ____ г.**

С целью реализации положений Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" в образовательной организации _____, приказываю:

1. Утвердить "План мероприятий по защите персональных данных образовательной организации" _____ согласно приложению № 1.
2. Создать комиссию для проведения мероприятий по защите персональных данных (далее – Комиссия) в составе:
   – председатель Комиссии – занимаемая должность и ФИО работника.

Члены комиссии:

   – должность и ФИО работника, выполняющего функции системного администратора;
   – должность и ФИО работника, выполняющего функции специалиста кадровой службы.
3. Комиссии:
   – провести классификацию информационных систем персональных данных в соответствии с установленной методикой;
   – составить перечень обрабатываемых в образовательной организации персональных данных;
   – разработать нормативные документы по защите персональных данных;
   – разработать формы учетных журналов;
   – привлечь для разработки модели актуальных угроз и вероятного нарушителя информационных систем персональных данных специализированную организацию, обладающую соответствующими лицензиями и квалифицированными специалистами.
4. Контроль за выполнением настоящего приказа оставляю за собой.

Директор образовательной организации
_____/_____/_____
(должность/подпись/Ф.И.О.)

С Приказом ознакомлены:
"___"_____ _____ г. _____ / _____
(подпись) (должность, Ф.И.О. работника)

"___"_____ _____ г. _____ / _____
(подпись) (должность, Ф.И.О. работника)

"___"_____ _____ г. _____ / _____
(подпись) (должность, Ф.И.О. работника)

ИСПОЛЬЗУЕМАЯ ЛИТЕРАТУРА

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» (Страсбург, 28 января 1981 г., с изменениями от 15 июня 1999 г., ETS № 108).
3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ.
4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
6. Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации».
7. Закон РФ от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
8. Закон РФ от 6.04.2011 № 63-ФЗ «Об электронной подписи».
9. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ».
10. Федеральный закон от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в РФ».
11. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».
12. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
13. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
14. Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

15. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
16. Постановление Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».
17. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (вместе с «Положением о лицензировании деятельности по технической защите конфиденциальной информации»).
18. Постановление Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
19. Распоряжение Правительства РФ от 25.04.2011 № 729-р «Об утверждении перечня услуг, оказываемых государственными и муниципальными учреждениями и другими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ), подлежащих включению в реестры государственных и муниципальных услуг и предоставляемых в электронной форме».
20. Распоряжение Правительства РФ от 17.12.2009 № 1993-р «Об утверждении сводного перечня первоочередных государственных и муниципальных услуг, предоставляемых в электронном виде».
21. Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».
22. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

23. Методические рекомендации по уведомлению уполномоченного органа о начале обработке персональных данных и о внесении изменений в ранее представленные сведения, утверждены приказом Роскомнадзора от 30.05.2017 № 94.
24. Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».
25. Приказ Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».
26. Письмо Роскомнадзора от 06.09.2022 № 08-80975 «О рассмотрении письма».
27. Письмо Роскомнадзора от 19.10.2021 № 08-71063 «О разъяснении законодательства».
28. Рекомендации по составлению документа, определяющего политику оператора в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».
29. Приказ Минобрнауки России от 17.05.2012 № 413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования».
30. Приказ Минобрнауки России от 25.12.2017 № 1259 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по профессии 08.01.05 Мастер столярно-плотничных и паркетных работ».
31. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
32. Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
33. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

34. Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».
35. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания 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 из уровней защищенности».
36. Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».
37. Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных».
38. Приказ Роскомнадзора от 30.05.2017 № 94 «Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения».
39. Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ»).
40. Приказ Роскомнадзора от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных"».
41. Приказ Минпросвещения России от 14.02.2022 № 74 «Об обработке и обеспечении защиты персональных данных в Министерстве просвещения

Российской Федерации» (вместе с «Правилами обработки персональных данных в Министерстве просвещения Российской Федерации», «Правилами рассмотрения запросов субъектов персональных данных или их представителей в Министерстве просвещения Российской Федерации», «Правилами осуществления в Министерстве просвещения Российской Федерации внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора», «Правилами работы с обезличенными данными в случае обезличивания персональных данных в Министерстве просвещения Российской Федерации», «Порядком доступа федеральных государственных гражданских служащих Министерства просвещения Российской Федерации в помещения, в которых ведется обработка персональных данных», «Должностным регламентом (должностными обязанностями) ответственного за организацию обработки персональных данных в Министерстве просвещения Российской Федерации»).

42. Письмо Рособразования от 29.07.2009 №17-110 «Об обеспечении защиты персональных данных».
43. Письмо Рособрнадзора от 12.04.2021 № 10-99 «О направлении методических документов, рекомендуемых при организации и проведении государствнной итоговой аттестации по образовательным программам основного общего и среднего общего образования в 2021 году».
44. Письмо> Минобрнауки России от 08.10.2015 № ВК-2569/07 «О направлении методических рекомендаций» (вместе с «Методическими рекомендациями по созданию и размещению в сети Интернет и средствах массовой информации видеосюжетов о детях, оставшихся без попечения родителей, а также иной производной информации указанной категории детей с целью реализации права детей жить и воспитываться в семье»)».
45. Письмо Минобрнауки России от 15.02.2012 № АП-147/07 «О методических рекомендациях по внедрению систем ведения журналов успеваемости в электронном виде».
46. «Типовые условия использования общедоступной информации, размещаемой в информационно-телекоммуникационной сети «Интернет» в форме открытых данных» (утв. протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от 19.09.2016 № 6).
47. Постановление Конституционного Суда РФ от 26.10.2017 № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального

закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова».

48. «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).

49. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».