Департамент образования города Москвы
Южный административный округ
Государственное бюджетное общеобразовательное учреждение
города Москвы «Школа № 1526 на Покровской»
(ГБОУ Школа № 1526 на Покровской)

117535, город Москва, ул. Дорожная, д. 20А
телефон/факс (495) 382-04-65, e-mail: 1526@edu.mos.ru, www.gymu**1526**.mskobr.ru
ОКПО 64518131, ОГРН 1097746830830, ИНН 7726643607, КПП 772601001

СОГЛАСОВАНО Председатель Управляющего совета ГБОУ Школы №1526 на Покровской _____ О.С. Кошелева 20.03.2018 года протокол № 4	СОГЛАСОВАНО на заседании Педагогического совета ГБОУ Школы №1526 на Покровской 19.03.2018 года протокол №	СОГЛАСОВАНО Председатель Профсоюзного комитета ГБОУ Школы №1526 на Покровской» _____ О.Б. Деревянных 19.03.2018 года протокол №	УТВЕРЖДАЮ Директор ГБОУ Школы №1526 на Покровской _____ К.К.Бадалян Приказ от 21.03.2018 года № 712 Регистрационный № 57

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 2017

Содержание

1. Введение **4**

2. Назначение и область действия **5**

3. Принципы и условия обработки персональных данных **6**

3.1 Принципы обработки персональных данных 6

3.2 Условия обработки персональных данных 6

4. Требования к обработке персональных данных **8**

4.1 Обязанности образовательной организации 8

4.2 Процессы обработки персональных данных 9

4.2.1 Сбор персональных данных 9

4.2.2 Использование персональных данных 10

4.2.3 Хранение персональных данных 10

4.2.4 Передача персональных данных 10

4.2.5 Уточнение персональных данных 11

4.2.6 Блокирование персональных данных 11

4.2.7 Уничтожение персональных данных 12

4.3 Обеспечение конфиденциальности персональных данных 13

4.4 Работа с персональных данных на автоматизированных рабочих местах 14

4.5 Работа с персональных данных, осуществляемая без использования средств автоматизации 14

4.6. Работа с обезличенными персональными данными 26

5. Взаимодействие с государственными органами **30**

6. Правила доступа к персональным данным **31**

7. Требования к работникам, допущенным к обработке персональных данных **33**

8. Ответственность за нарушения при обработке персональных данных **20**

1. Введение

1.1 Настоящее Положение разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных, в том числе при их обработке в информационных системах персональных данных.

1.2 Основными нормативно-правовыми документами, на которых базируется настоящее Положение, являются:

– Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), устанавливающий основные принципы и условия обработки персональных данных, права, обязанности и ответственность участников отношений, связанных с обработкой персональных данных;

– Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.3 Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных, обработки обращений субъектов персональных данных и взаимодействия с уполномоченным органом по защите прав субъектов персональных данных (Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, Роскомнадзор) приказом директора ГБОУ Школы № 1526 на Покровской (далее – образовательная организация) назначается работник, ответственный за организацию обработки персональных данных, и работник, ответственный за обеспечение безопасности персональных данных.

1.4 Настоящее Положение подлежит пересмотру и при необходимости актуализации в случае изменений в законодательстве Российской Федерации о персональных данных, при изменении организационной структуры образовательной организации.

2.Назначение и область действия

2.1 Настоящее Положение предназначено для организации в образовательной организации процесса обработки персональных данных согласно нормам и принципам действующего федерального законодательства.

2.2 Действие настоящего Положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению персональных данных, осуществляемые с использованием средств автоматизации и без их использования.

2.3 Положение обязательно для ознакомления и исполнения всеми работниками, допущенными к обработке персональных данных, Ответственным за организацию обработки персональных данных, Ответственным за обеспечение безопасности персональных данных, инженерами по телекоммуникации (техниками).

3. Принципы и условия обработки персональных данных

3.1 Принципы обработки персональных данных

3.1.1 Обработка персональных данных должна осуществляться на основе следующих принципов:

1) законности целей и способов обработки персональных данных и добросовестности;

2) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;

3) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

4) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

5) недопустимости объединения созданных для несовместимых между собой целей обработки баз данных информационных систем персональных данных.

3.1.2 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

3.2 Условия обработки персональных данных

3.2.1 Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных законодательством, в частности:

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональных данных которых подлежат обработке, а также определяющего полномочия оператора;

2) обработка персональных данных осуществляется в целях исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для осуществления прав и законных интересов учреждения как оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

3.2.2 В следующих случаях требуется дополнительное письменное согласие субъекта на обработку его персональных данных:

1) включение персональных данных субъекта в общедоступные источники персональных данных;

2) обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

3) обработка биометрических персональных данных (сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность);

4) трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных[1];

5) принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

3.2.3 Обработка специальных категорий персональных данных допускается без письменного согласия субъекта в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что такая обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

3.2.4 В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

3.2.5 В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

3.2.6 При отсутствии необходимости письменного согласия субъекта на обработку его персональных данных в форме, определенной законодательством, для возможности доказательства получения согласия субъекта на обработку его персональных данных рекомендуется брать согласие субъекта в произвольной форме. Примером такого согласия может служить поле для подписи субъекта персональных данных (либо для проставления субъектом галочки) и текст рядом с этим полем: «Даю ГБОУ Школе № 1526 на Покровской свое согласие на обработку своих персональных данных с целью _____ на срок _____/ до момента отзыва данного согласия».

3.2.7 Для каждого процесса образовательной организации, в рамках которого производится обработка персональных данных, и для осуществления которого требуется письменное согласие субъекта персональных данных, по приведенной форме составляется отдельный шаблон согласия на обработку с указанием целей обработки персональных данных в рамках данного процесса, видов персональных данных и необходимого периода их хранения.

3.2.8 В случае если образовательная организация на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также обязательное указание целей передачи персональных данных и перечня видов передаваемых на обработку персональных данных.

3.2.9 Образовательной организацией и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

[1] Адекватную защиту ПДи обеспечивают страны, подписавшие и ратифицировавшие Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иные иностранные государства, обеспечивающие адекватную защиту прав субъектов персональных данных в соответствии с ФЗ «О персональных данных»

4. Требования к обработке персональных данных

4.1 Обязанности образовательной организации

4.1.1 В соответствии с требованиями Закона о персональных данных образовательная организация обязана:

1) предоставлять субъекту персональных данных (законному представителю субъекта) по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставлять отказ в течение тридцати дней[2] с даты получения запроса субъекта персональных данных или его представителя;

2) уточнять обрабатываемые персональных данных по требованию субъекта персональных данных (законного представителя субъекта), блокировать или удалять, если персональных данных являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки в срок, не превышающий семи рабочих дней[3] со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих эти факты;

3) вести журнал учета обращений субъектов персональных данных (законных представителей субъекта), в котором должны фиксироваться запросы субъектов персональных данных (законных представителей субъектов) на получение персональных данных, а также факты предоставления персональных данных по этим запросам;

4) уведомлять субъекта персональных данных об обработке его персональных данных в том случае, если персональных данных были получены не от субъекта персональных данных (за исключением случаев, оговоренных в подразделе 4.2.1 ниже);

5) в случае достижения цели обработки персональных данных незамедлительно прекращать обработку персональных данных и уничтожать соответствующие персональных данных в срок, не превышающий тридцати дней[4], если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между образовательная организациям и субъектом персональных данных, либо если образовательная организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами;

6) в случае отзыва субъектом персональных данных (законным представителем субъекта) согласия на обработку своих персональных данных (персональных данных представляемого лица) прекратить обработку персональных данных и уничтожить персональных данных в следующие сроки:

– в срок, не превышающий тридцати дней[5] с даты достижения цели обработки персональных данных, в соответствии с согласием субъекта на обработку его персональных данных;

– в срок, не превышающий тридцати дней[6], если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между образовательной организацией и субъектом персональных данных, либо если образовательная организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных ФЗ «О персональных данных» или другими федеральными законами;

7) уведомлять субъекта персональных данных об уничтожении его персональных данных;

8) немедленно прекратить обработку персональных данных субъекта персональных данных в случае поступления требования субъекта персональных данных (законного представителя) о

[2] Ст. 20 ч. 1, 2 ФЗ «О персональных данных»
[3] Ст. 21 ч. 2 ФЗ «О персональных данных»
[4] Ст. 21 ч. 4 ФЗ «О персональных данных»
[5] Ст. 21 ч. 5 ФЗ «О персональных данных»
[6] Ст. 21 ч. 4 ФЗ «О персональных данных»

прекращении обработки его персональных данных в целях продвижения товаров, работ, услуг на рынке.

4.1.2 В случае если образовательная организация является уполномоченным лицом по обработке персональных данных, субъект имеет право написать обращение оператору, а оператор со своей стороны должен перенаправить обращение в образовательную организацию.

4.2 Процессы обработки персональных данных

Обработка персональных данных в информационных системах персональных данных включает в себя следующие основные процессы:

– сбор персональных данных;
– использование персональных данных;
– хранение персональных данных в информационных системах персональных данных;
– передача персональных данных;
– уточнение персональных данных;
– блокирование персональных данных;
– уничтожение персональных данных.

4.2.1 Сбор персональных данных

4.2.1.1 Персональные данные получаются лично у субъектов персональных данных (законных представителей субъектов) либо от другого оператора, за исключением случаев получения персональных данных из общедоступных источников (в том числе справочников, адресных книг).

4.2.1.2 При сборе персональных данных образовательная организация обязана использовать базы данных, находящиеся на территории Российской Федерации.

4.2.1.3 В случаях, когда персональные данные получены не от субъекта персональных данных, то до начала обработки таких персональных данных субъекту персональных данных предоставляется следующая информация:

– наименование и адрес образовательной организации;
– цель обработки персональных данных и ее правовое основание;
– предполагаемые пользователи персональных данных;
– установленные Законом о персональных данных права субъекта персональных данных;
– источник получения персональных данных.

4.2.1.4 Уведомление субъекта об обработке персональных данных, полученных не от него самого, не осуществляется в следующих случаях:

– субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

– персональные данные получены на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

– персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

– образовательная организация осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных.

4.2.1.5 Образовательная организация может получать, обрабатывать и приобщать к личному делу работников и обучающихся данные о состоянии их здоровья без письменного согласия, когда обработка персональных данных осуществляется или необходима:

– в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;

– для защиты жизни, здоровья или иных жизненно важных интересов работника образовательной организации либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно;

– для установления или осуществления прав персональных данных работника образовательной организации или третьих лиц, а равно и в связи с осуществлением правосудия;

– в соответствии с законодательством об обязательных видах страхования и со страховым законодательством.

4.2.1.6 Во всех остальных случаях образовательная организация может получать, обрабатывать и приобщать к личному делу работников и обучающихся данные о состоянии их здоровья только с их письменного согласия (согласия законных представителей).

4.2.2 Использование персональных данных

Использование персональных данных, собранных в соответствии с подразделом 4.2.1 выше, в информационных системах персональных данных осуществляется работниками, занимающими должности, допущенные приказом директора образовательной организации к работе с персональными данными, в целях принятия решений или совершения иных действий в отношении субъекта персональных данных и обеспечения функционирования процессов образовательной организации.

4.2.3 Хранение персональных данных

4.2.3.1 Хранение персональных данных в образовательной организации осуществляется в соответствии со следующими требованиями:

– хранение персональных данных осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места их хранения;

– хранение персональных данных осуществляется 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;

– не осуществляется несанкционированное копирование персональных данных на отчуждаемые носители информации;

– при хранении персональных данных в информационных системах персональных данных соблюдаются условия, обеспечивающие конфиденциальность и сохранность персональных данных;

– исключен несанкционированный доступ к персональных данных (доступ разрешен только работникам образовательной организации, включенным в перечень должностей работников образовательной организации, допущенных к работе с персональными данными).

4.2.3.2 Работники образовательной организации, обладающие правом доступа к персональным данным, несут ответственность за хранение персональных данных на своих автоматизированных рабочих местах.

4.2.3.3 Копирование персональных данных на внешние электронные носители, такие как флеш-накопители, внешние жесткие диски, CD, DVD и т. д. осуществляется только для выполнения трудовых обязанностей и требований нормативных правовых актов.

4.2.4 Передача персональных данных

4.2.4.1 Передача персональных данных другим работникам образовательной организации или третьим лицам осуществляется в следующих случаях:

– исполнение работником трудовых обязанностей, связанных с обработкой персональных данных;

– передача персональных данных организациям, с которыми заключены договоры, предполагающие передачу и обработку персональных данных, в целях обеспечения процессов образовательной организации;

– передача персональных данных в рамках исполнения федерального законодательства.

4.2.4.2 Работники образовательной организации, допущенные к работе с персональных данных, не сообщают устно или письменно персональные данные другим работникам или сторонним лицам, которые не участвуют в процессах обработки персональных данных.

4.2.4.3 Ответы на письменные запросы других организаций и учреждений в пределах их компетенции и предоставленных полномочий даются в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных данных.

4.2.4.4 При передаче персональных данных работники образовательной организации не сообщают персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы

жизни и здоровью субъекта персональных данных, а также в случаях, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами.

4.2.4.5 Передача персональных данных возможна только в том случае, если исключен несанкционированный доступ к персональных данных в процессе передачи и обеспечивается конфиденциальность передаваемой информации. Если образовательная организация на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их передаче.

4.2.4.6 Согласие субъекта на передачу его персональных данных не требуется, если сообщение информации или предоставление документов, содержащих персональные данные, предусмотрено законодательством Российской Федерации.

4.2.4.7 Работники образовательной организации осуществляют передачу персональных данных субъекта персональных данных представителю субъекта персональных данных, проверив его полномочия в порядке, установленном законодательством Российской Федерации, и ограничиваются только теми персональными данными, которые необходимы для выполнения указанными представителями функций.

4.2.4.8 В случаях поручения обработки персональных данных другому лицу образовательная организация заключает поручение оператора с этим лицом, существенным условием которого является обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

4.2.4.9 До начала осуществления трансграничной передачи персональных данных образовательная организация обязана убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.

4.2.4.10 Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

– наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

– предусмотренных международными договорами Российской Федерации.

4.2.4.11 Документы, содержащие персональные данные, передаются через организации, специализирующиеся на почтовых рассылках, организацию федеральной почтовой связи, а также лично работникам сторонних организаций под подпись.

4.2.4.12 Электронные документы, содержащие персональные данные, передаются на учтенных носителях информации и (или) по телекоммуникационным каналам связи при использовании средств криптографической защиты информации.

4.2.5 Уточнение персональных данных

4.2.5.1 В случае выявления работником образовательной организации недостоверных персональных данных или неправомерных действий с ними работник информирует о данном факте Ответственного за организацию обработки персональных данных. Ответственный за организацию обработки персональных данных в срок, не превышающий трех рабочих дней[7] с даты этого выявления, инициирует выполнение действий, описанных в документе «Порядок обработки обращений субъектов персональных данных».

4.2.5.2 В случае уточнения (изменения) персональных данных необходимо известить третьих лиц, которым ранее были сообщены или переданы неверные или неполные персональные данные, обо всех исключениях, исправлениях и дополнениях в них.

4.2.5.3 Об устранении допущенных нарушений или об уничтожении персональных данных требуется уведомить субъекта персональных данных или его законного представителя либо уполномоченный орган по защите прав субъектов персональных данных в случае, если соответствующую проверку инициировал указанный орган.

4.2.6 Блокирование персональных данных

[7] Ст. 21 ч. 3 ФЗ «О персональных данных»

4.2.6.1 В случае выявления работником образовательной организации неправомерной обработки персональных данных или выявления неточных персональных данных при обращении субъекта или его представителя либо по запросу уполномоченного органа по защите прав субъектов персональных данных Ответственный за организацию обработки персональных данных инициирует блокирование персональных данных, относящихся к этому субъекту персональных данных, и выполнение действий, описанных в документе «Порядок обработки обращений субъектов персональных данных».

4.2.6.2 В случаях, если отсутствует возможность уничтожения персональных данных, образовательная организация осуществляет блокирование таких персональных данных и обеспечивает их уничтожение в срок, не превышающий шести месяцев.

4.2.7 Уничтожение персональных данных

4.2.7.1 Персональные данные подлежат уничтожению (или обезличиванию) в следующих случаях в указанные сроки:

– по достижении целей обработки персональных данных – в 30-дневный срок[8];

– в случае утраты необходимости в достижении целей обработки персональных данных – в 30-дневный срок[9];

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных – в 30-дневный[10] срок, если иной срок не предусмотрен договором или соглашением между образовательной организацией и субъектом персональных данных либо если образовательная организация не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами.

4.2.7.2 Персональные данные подлежат уничтожению (или обезличиванию) в срок, не превышающий десяти рабочих дней[11] с даты выявления неправомерной обработки персональных данных, в следующих случаях:

– в случае если персональные данные являются неполными, устаревшими, неточными (при условии, что уточнение персональных данных невозможно);

– в случае если персональные данные являются незаконно полученными;

– в случае если персональные данные не являются необходимыми для заявленной цели обработки.

4.2.7.3 Процесс уничтожения персональных данных при достижении целей их обработки либо в случае утраты необходимости в достижении этих целей инициирует владелец процесса, в котором эти персональные данные обрабатываются.

4.2.7.4 Процесс уничтожения персональных данных инициирует Ответственный за организацию обработки персональных данных.

4.2.7.5 Владелец процесса, в котором обрабатываются персональные данные, согласовывает уничтожение персональных данных с Ответственным за организацию обработки персональных данных в служебной записке.

4.2.7.6 Ответственный за организацию обработки персональных данных на основании информации, указанной в Перечне персональных данных, обрабатываемых в образовательной организации, определяет, в каких еще бизнес-процессах и в каких информационных системах персональных данных осуществляется обработка персональных данных.

4.2.7.7 Ответственный за организацию обработки персональных данных назначает лицо, ответственное за уничтожение персональных данных. В случае с бумажными носителями персональных данных в качестве лица, ответственного за уничтожение персональных данных, назначается владелец процесса. В случае с другими носителями персональных данных или если обработка персональных данных осуществляется в информационных системах персональных данных, в качестве лица, ответственного за уничтожение персональных данных, назначается

[8] Ст. 21 ч. 4 ФЗ «О персональных данных»
[9] Ст. 21 ч. 4 ФЗ «О персональных данных»
[10] Ст. 21 ч. 5 ФЗ «О персональных данных»
[11] Ст. 21 ч. 3 ФЗ «О персональных данных»

инженер по телекоммуникациям (техник) или работник, ответственный за эксплуатацию информационной системы персональных данных.

4.2.7.8 Лицо, ответственное за уничтожение персональных данных, производит уничтожение персональных данных, оформляет и подписывает акт об уничтожении персональных данных. После этого он направляет акт об уничтожении персональных данных Ответственному за организацию обработки персональных данных.

4.2.7.9 Ответственный за организацию обработки персональных данных утверждает акт об уничтожении персональных данных и уведомляет субъекта персональных данных или его представителя.

4.2.7.10 В случае уничтожения персональных данных по результатам проверки или запроса уполномоченного органа по защите прав субъектов персональных данных Ответственный за организацию обработки персональных данных уведомляет об уничтожении персональных данных субъекта персональных данных или его представителя, а также указанный орган.

4.2.7.11 В случае отсутствия возможности уничтожения персональных данных в течение сроков, указанных в пунктах 4.2.7.1 и 4.2.7.2 выше, персональные данные должны быть заблокированы, после чего персональные данные должны быть уничтожены в срок, не превышающий шести месяцев.

4.2.7.12 При уничтожении обеспечивается гарантированное уничтожение персональных данных, исключающее возможность их восстановления программными или физическими методами.

4.2.7.13 Уничтожение бумажных носителей персональных данных производится собственными силами образовательной организации или с привлечением специализированной организации путем измельчения, сжигания или преобразования в целлюлозную массу таким образом, чтобы гарантировать невозможность их восстановления.

4.2.7.14 Уничтожение персональных данных в ручном режиме должно оформляться актом об уничтожении персональных данных.

4.3 Обеспечение конфиденциальности персональных данных

4.3.1 Образовательная организация и иные лица, обладающие правом доступа к персональных данных (в рамках выполнения должностных обязанностей или в рамках договора), исполняют обязательство не раскрывать третьим лицам и не распространять персональных данных без согласия субъекта персональных данных, если иное не предусмотрено Законом о персональных данных.

4.3.2 Для обеспечения безопасности персональных данных от неправомочных действий выполняются следующие организационные меры:

– повышение осведомленности работников образовательной организации по вопросам обеспечения безопасности персональных данных при их обработке;

– своевременное выявление нарушений работниками требований к режиму конфиденциальности;

– все работники, имеющие действующие трудовые отношения, деятельность которых связана с получением и обработкой персональных данных, подписывают обязательство о неразглашении персональных данных либо заключают дополнительное соглашение к трудовым договорам, а также ознакомляются под подпись с настоящим Положением;

– со всеми принимаемыми на работу работниками, деятельность которых будет связана с обработкой персональных данных, заключаются трудовые договоры, и с этими работниками подписываются соответствующие должностные инструкции, в которых должны быть отражены вопросы обязанности обеспечения конфиденциальности персональных данных;

– разделение полномочий пользователей в информационных системах персональных данных в зависимости от их должностных обязанностей;

– наличие формализованной процедуры по предоставлению доступа к информационным системам персональных данных, а также по регулярному пересмотру (ревизии) прав доступа работников образовательной организации в зависимости от занимаемой ими должности.

4.3.3 Образовательная организация передает персональные данные на обработку третьим лицам (принимающей стороне), только если это необходимо для достижения целей обработки персональных данных, причем существенным условием договора является обязанность

обеспечения третьей стороной конфиденциальности и безопасности персональных данных при их обработке.

4.3.4 Передача персональных данных третьим лицам без заключенного договора и без применения мер защиты персональных данных не осуществляется.

4.4 Работа с персональных данных на автоматизированных рабочих местах

При работе с персональными данными на автоматизированных рабочих местах работники образовательной организации соблюдают следующие правила:

– принятые в образовательной организации правила парольной политики;

– исключение возможности подсматривания информации на мониторе посторонними лицами, в том числе и с помощью технических средств (стационарных и встроенных в мобильные телефоны фото- и видеокамер и т. п.);

– блокирование компьютера при покидании рабочего места в течение рабочего дня даже на небольшой период времени.

4.5 Работа с персональными данными, осуществляемая без использования средств автоматизации

4.5.1 Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

4.5.2 При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

4.5.3 Работники, осуществляющие обработку персональных данных без использования средств автоматизации, до начала обработки информируются Ответственным за организацию обработки персональных данных о факте обработки ими персональных данных, о категориях персональных данных, об особенностях и правилах обработки персональных данных.

4.5.4 В типовую форму, в которую происходит внесение персональных данных, включается следующая информация:

– цель обработки персональных данных, наименование и адрес образовательной организации, источник получения персональных данных, срок обработки персональных данных, перечень действий с персональных данных, которые будут совершаться в процессе их обработки;

– поле для проставления субъектом персональных данных отметки о согласии на обработку персональных данных без использования средств автоматизации.

4.5.5 Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

4.5.6 Копирование информации, содержащейся в журнале учета посетителей, не допускается.

4.5.7 Персональные данные каждого субъекта персональных данных заносятся в журнал учета посетителей не более одного раза в каждом случае пропуска субъекта персональных данных на территорию образовательной организации.

4.5.8 При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

– при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

4.5.9 Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

4.5.10 Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

4.5.11 Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.5.12 В образовательной организации осуществляется раздельное хранение персональных данных (материальных носителей), обработка которых совершается в различных целях.

4.5.13 Материальные носители с персональными данными не оставляются без присмотра. Лица, ответственные за носители персональных данных, при покидании рабочего места убирают носители персональных данных в сейф или шкаф, закрывающийся на ключ. Кабинеты, в которых хранятся документы, содержащие персональные данные, при покидании их работниками образовательной организации запираются.

4.6 Работа с обезличенными персональными данными

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

4.6.2 Обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки. Для этого обезличенные данные должны обладать свойствами, сохраняющими основные характеристики обезличиваемых персональных данных.

4.6.3 К свойствам обезличенных данных относятся:

– полнота (сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания);

– структурированность (сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания);

– релевантность (возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме);

– семантическая целостность (сохранение семантики персональных данных при их обезличивании);

– применимость (возможность решения задач обработки персональных данных, стоящих перед образовательной организацией, осуществляющей обезличивание персональных данных,);

– анонимность (невозможность однозначной идентификации субъектов персональных данных, полученных в результате обезличивания, без применения дополнительной информации).

4.6.4 К характеристикам (свойствам) методов обезличивания персональных данных, определяющим возможность обеспечения заданных свойств обезличенных данных, относятся:

- обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность);

- вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);

- изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);

- стойкость (стойкость метода к атакам на идентификацию субъекта персональных данных);

- возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);

- совместимость (возможность интеграции персональных данных, обезличенных различными методами);

- параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);

- возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).

4.6.5 Требования к методам обезличивания подразделяются:

- на требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;

- требования к свойствам, которыми должен обладать метод обезличивания.

4.6.6 К требованиям к свойствам получаемых обезличенных данных относятся:

- сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);

- сохранение структурированности обезличиваемых персональных данных;

- сохранение семантической целостности обезличиваемых персональных данных;

- анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).

4.6.7 К требованиям к свойствам метода обезличивания относятся:

- обратимость (возможность проведения деобезличивания);

- возможность обеспечения заданного уровня анонимности;

- увеличение стойкости при увеличении объема обезличиваемых персональных данных.

4.6.8 Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.

4.6.9 Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

4.6.10 При обработке обезличенных персональных данных соблюдаются требования внутренних нормативных документов, регламентирующих обработку и защиту необезличенных персональных данных.

4.6.11 Используемые процедуры обезличивания и деобезличивания персональных данных должны соответствовать условиям и целям обработки персональных данных.

4.6.12 Обезличивание, деобезличивание и обработка обезличенных данных не должны нарушать права субъекта персональных данных.

4.6.13 Обезличивание персональных данных субъектов осуществляется перед внесением их в информационную систему.

4.6.14 Метод обезличивания персональных данных, обезличенные персональные данные и сопутствующие им сведения, позволяющие провести деобезличивание персональных данных, не подлежат разглашению и нарушению конфиденциальности.

4.6.15 Не допускается совместное хранение обезличенных данных и служебной информации о реализованном методе обезличивания и параметрах процедуры.

4.6.16 Совместная передача обезличенных данных и служебной информации о реализованном методе обезличивания и параметрах процедуры допускается только при обеспечении конфиденциальности канала связи.

4.6.17 Деобезличенные данные, полученные в процессе обработки обезличенных данных, подлежат уничтожению.

5.Взаимодействие с государственными органами

5.1 Образовательная организация обязана уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, указанных в Порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных.

5.2 Образовательная организация сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней[12] с даты получения запроса.

5.3 В случае получения запроса или обращения уполномоченного органа по защите прав субъектов персональных данных о недостоверности персональных данных или неправомерных действиях с ними выявленные нарушения подлежат исправлению. Образовательная организация сообщает в указанный орган об устранении нарушений либо об уничтожении персональных данных в случае невозможности устранения нарушений в срок, не превышающий десяти рабочих дней[13].

5.4 В установленных федеральным законодательством случаях образовательная организация предоставляет информацию, содержащую обрабатываемые персональные данные, по мотивированному запросу уполномоченных органов государственной власти по вопросам их компетенции.

5.5 Запросы на предоставление доступа к обрабатываемым персональным данным могут быть обжалованы в судебном порядке в соответствии с законодательством Российской Федерации.

5.6 Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных описан в Порядке взаимодействия с уполномоченным органом по защите прав субъектов персональных данных.

[12] Ст. 20 ч. 4 ФЗ «О персональных данных»
[13] Ст. 22 ч. 7 ФЗ «О персональных данных»

6. Правила доступа к персональным данным

6.1 В образовательной организации Ответственным за обработку персональных данных на основании предоставленных руководителями подразделений списков должностей, допущенных к обработке персональных данных, разрабатывается Перечень должностей работников, допущенных к работе с персональными данными, определяющий связь между должностями работников и персональными данными, к которым предоставляется доступ. Этот перечень подлежит пересмотру и при необходимости актуализации не реже одного раза в год.

6.2 Работникам образовательной организации предоставляется доступ к работе с персональными данными исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

6.3 Работники образовательной организации, которые в силу выполняемых должностных обязанностей постоянно работают с персональными данными, получают допуск к необходимым категориям персональных данных с установленными правами доступа на срок выполнения ими соответствующих должностных обязанностей на основании Перечня должностей работников, допущенных к работе с персональными данными, который утверждается директором образовательной организации по представлению Ответственного за обеспечение безопасности персональных данных.

6.4 Перечень должностей работников, допущенных к работе с персональными данными, поддерживается в актуальном состоянии. С этой целью проводятся следующие мероприятия:

– на основании согласованных заявок на предоставление доступа Ответственным за организацию обработки персональных данных формируется Перечень должностей работников, допущенных к работе с персональными данными для выполнения своих должностных обязанностей;

– каждые полгода Перечень должностей работников, допущенных к работе с персональными данными, актуализируется Ответственным за организацию обработки персональных данных путем анализа категорий работников, которым необходим доступ к персональным данным.

6.5 Временный или разовый допуск к работе с персональными данными в связи со служебной необходимостью может быть получен работником образовательной организации по согласованию с Ответственным за обеспечение безопасности персональных данных путем подачи заявки на доступ с указанием цели и срока доступа и категорий персональных данных, к которым запрашивается доступ.

6.6 Доступ к персональным данным может быть прекращен или ограничен в случае нарушения требований настоящего Положения либо в случае изменения должностных обязанностей или увольнения работника образовательной организации.

6.7 Предоставление и прекращение доступа пользователей к персональным данным осуществляется ответственными за эксплуатацию соответствующих информационных систем персональных данных[14].

[14] Ответственным за эксплуатацию централизованных систем Департамента образования г. Москвы является директор образовательной организации, в задачи которого входит своевременное направление официальных обращений в Департамент информационных технологий г. Москвы, непосредственно осуществляющий предоставление и прекращение доступа пользователей к централизованным системам; для нецентрализованных систем, функционирующих в пределах образовательной организации, ответственный из числа работников назначается директором образовательной организации

7.Требования к работникам, допущенным к обработке персональных данных

7.1 Все работники образовательной организации, которым стали известны персональные данные, обрабатывающиеся в информационных системах персональных данных образовательной организации, должны обеспечивать их конфиденциальность.

7.2 Все работники образовательной организации, допущенные к работе с персональными данными, ознакомлены под подпись с требованиями настоящего Положения.

7.3 Работники, ответственные за организацию работы подразделений, работниками которых производится обработка персональных данных, а также Ответственный за обеспечение безопасности персональных данных должны быть под подпись ознакомлены с требованиями настоящего документа.

7.4 В образовательной организации организован процесс обучения работников, допущенных к работе с персональными данными, по направлению обеспечения безопасности персональных данных. Ответственность за процесс обучения возлагается на Ответственного за организацию обработки персональных данных.

7.5 Трудовые договоры (или должностные инструкции) работников образовательной организации, допущенных к работе с персональными данными, содержат раздел, описывающий персональную ответственность за нарушение требований по обеспечению безопасности персональных данных, включая нарушение свойств целостности, конфиденциальности, доступности и установленного порядка обработки персональных данных.

7.6 В случае нарушения установленного порядка обработки персональных данных работники образовательной организации несут ответственность в соответствии с разделом 8настоящего Положения.

8. Ответственность за нарушения при обработке персональных данных

8.1 Работники образовательной организации несут персональную ответственность за соблюдение требований по обработке и обеспечению безопасности персональных данных, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

8.2 Работник образовательной организации может быть привлечен к ответственности в случаях:

– умышленного или неосторожного раскрытия персональных данных;

– утраты материальных носителей, содержащих персональные данные (материальные носители персональных данных);

– нарушения требований настоящего Положения и других локальных нормативных актов в части вопросов обработки персональных данных.

8.3 В случае нарушения установленного порядка обработки и обеспечения безопасности персональных данных, несанкционированного доступа к персональных данных, раскрытия персональных данных и нанесения образовательной организации, его работникам, клиентам, посетителям и другим субъектам персональных данных материального или иного ущерба виновные лица несут предусмотренную законодательством Российской Федерации ответственность.