

Приложение № 3 к приказу
ГАОУ ДПО «Корпоративный
университет»

от «06» 09 2021 г.

№ 164/02

ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 2021

Содержание

1 Введение.....	3
2 Назначение и область действия.....	4
3 Принципы и условия обработки персональных данных	5
3.1 Принципы обработки персональных данных.....	5
3.2 Условия обработки персональных данных	5
4 Требования к обработке персональных данных	8
4.1 Обязанности Учреждения	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	11
4.2.5 Уточнение персональных данных.....	12
4.2.6 Блокирование персональных данных	13
4.2.7 Уничтожение персональных данных.....	13
4.3 Обеспечение конфиденциальности персональных данных.....	15
4.4 Работа с персональными данными на автоматизированных рабочих местах.....	16
4.5 Работа с персональными данными, осуществляемая без использования средств автоматизации.....	16
5 Взаимодействие с государственными органами	26
6 Правила доступа к персональным данным	28
7 Требования к работникам, допущенным к обработке персональных данных.....	30
8 Ответственность за нарушения при обработке персональных данных	22

1 Введение

1.1 Настоящее Положение разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иным законодательством Российской Федерации о персональных данных и правовыми актами федеральных органов исполнительной власти по вопросам обеспечения безопасности персональных данных, в том числе при их обработке в информационных системах персональных данных.

1.2 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 приказом директора Государственного автономного образовательного учреждения дополнительного профессионального образования города Москвы «Корпоративный университет московского образования» (далее – Учреждение) назначается работник, ответственный за организацию обработки персональных данных в Учреждении, и работник, ответственный за обеспечение безопасности персональных данных.

1.3 Настоящее Положение подлежит актуализации в случае изменений в законодательстве Российской Федерации о персональных данных и/или при изменении организационной структуры Учреждения.

2 Назначение и область действия

2.1 Настоящее Положение предназначено для организации в Учреждении процесса обработки персональных данных согласно нормам и принципам законодательства Российской Федерации.

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, работнику, ответственному за организацию обработки персональных данных, работнику, ответственному за обеспечение безопасности персональных данных, инженерами по телекоммуникации (техниками), а также их руководителям.

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;
- 2) добросовестности;
- 3) соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- 4) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- 5) достоверности персональных данных;
- 6) 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 осуществляется оператором с согласия субъектов персональных данных, за исключением случаев, предусмотренных законодательством, в частности:

- 1) 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;
- 2) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- 3) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- 4) 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 Дополнительное письменное согласие субъекта на обработку его персональных данных требуется в случаях:

- 1) включения персональных данных субъекта в общедоступные источники персональных данных;
- 2) обработки специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

3) обработки биометрических персональных данных (сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность), за исключением случаев, когда обработка ведется в рамках целей, определенных в пункте 2 части 1 статьи 6 и части 2 статьи 11 Закона о персональных данных, Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции», Трудовым кодексом Российской Федерации;

4) трансграничной передачи персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных¹;

5) принятия 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 с 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 ГАОУ ДПО «Корпоративный университет» свое согласие на обработку своих персональных данных с целью _____ на срок _____ / до момента отзыва данного согласия».

3.2.7 Для каждого процесса Учреждения, 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.

¹ Адекватную защиту ПДн 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 Законом о персональных данных

3.2.8 В случае если Учреждение на основании договора поручает обработку персональных данных другому лицу, существенным условием такого 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 Учреждением и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

4 Требования к обработке персональных данных

4.1 Обязанности Учреждения

4.1.1 В соответствии с требованиями Закона о персональных данных Учреждение обязано:

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 дней² с даты получения запроса субъекта персональных данных или его представителя;

2) уточнять обрабатываемые персональные данные по требованию субъекта персональных данных (законного представителя субъекта), блокировать или удалять персональные данные, если они являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки персональных данных, в срок, не превышающий семи рабочих дней³ 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 и факты отказа в предоставлении персональных данных по этим запросам;

4) уведомлять субъекта персональных данных об обработке его персональных данных в том случае, если персональные данные были получены не от субъекта персональных данных;

5) в случае достижения цели обработки персональных данных незамедлительно прекращать обработку персональных данных и уничтожать соответствующие персональные данные в срок, не превышающий тридцати дней⁴, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение 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 персональные данные:

– в срок, не превышающий тридцати дней⁵ с даты достижения цели обработки персональных данных, в соответствии с согласием субъекта на обработку его персональных данных;

– в срок, не превышающий тридцати дней⁶, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому

² Ст. 20 ч. 1, 2 Закон о персональных данных

³ Ст. 21 ч. 2 Закон о персональных данных

⁴ Ст. 21 ч. 4 Закон о персональных данных

⁵ Ст. 21 ч. 5 Закон о персональных данных

⁶ Ст. 21 ч. 4 Закон о персональных данных

является субъект персональных данных, иным соглашением между Учреждением и субъектом персональных данных, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом 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 прекращении обработки его персональных данных в целях продвижения товаров, работ, услуг на рынке.

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

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 Учреждение обязано 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 Учреждения;
- 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;
- Учреждение 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 Учреждение 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 случаях, предусмотренных законодательством о государственной социальной помощи, трудовым законодательством, пенсионным законодательством Российской Федерации;
- в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, при наличии в штате Учреждения лица, профессионально занимающегося медицинской деятельностью и обязанного в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- в целях защиты жизни, здоровья или иных жизненно важных интересов работника либо для защиты жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;
- в целях установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;
- в случаях, предусмотренных законодательством об обязательных видах страхования, страховым законодательством, об обороне, о противодействии коррупции и иным специальным законодательством.

4.2.1.6 Во всех остальных случаях Учреждение 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 пунктом 4.2.1, в информационных системах персональных данных осуществляется работниками, занимающими должности, допущенные приказом директора Учреждения к работе с персональными данными, в целях принятия решений или совершения иных действий в отношении субъекта персональных данных и обеспечения функционирования процессов Учреждения.

4.2.3 Хранение персональных данных

4.2.3.1 Хранение персональных данных в Учреждении 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 персональным данным (доступ разрешен только работникам Учреждения, включенным в перечень должностей работников Учреждения, допущенных к работе с персональными данными).

4.2.3.2 Работники Учреждения, 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 Учреждения 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 Учреждения;

– передача персональных данных в рамках исполнения федерального законодательства.

4.2.4.2 Работники Учреждения, допущенные к работе с персональными данными, 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 Учреждения 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 персональным данным в процессе передачи и обеспечивается конфиденциальность передаваемой информации. Если Учреждение 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 Учреждения 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 указанных представителем функций.

4.2.4.8 В случаях поручения обработки персональных данных другому лицу Учреждение заключает соглашение 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 Учреждение обязано 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 – уполномоченным работникам сторонних организаций под подпись.

4.2.4.12 Электронные документы, содержащие персональные данные, передаются на учетных 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 Учреждения недостоверных персональных данных или неправомерных действий с ними он информирует о данном факте Ответственного за организацию обработки персональных данных. Ответственный за организацию обработки персональных данных в срок, не

превышающий трех рабочих дней⁷ с даты этого выявления, инициирует выполнение действий, описанных в Порядке 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

4.2.6.1 В случае выявления работником Учреждения 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.

4.2.6.2 В случаях, если отсутствует возможность уничтожения персональных данных, Учреждение осуществляет блокирование таких персональных данных и обеспечивает их уничтожение в срок, не превышающий шести месяцев, если иной срок не установлен федеральными законами. Обоснование невозможности уничтожения персональных данных в установленные законодательством сроки должно быть документально оформлено.

4.2.7 Уничтожение персональных данных

4.2.7.1 Персональные данные подлежат уничтожению (или обезличиванию):

- по достижении целей обработки персональных данных – в 30-дневный срок⁸;
- в случае утраты необходимости в достижении целей обработки персональных данных – в 30-дневный срок⁹;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных – в 30-дневный¹⁰ срок, если иной срок не предусмотрен договором или соглашением между Учреждением и субъектом персональных данных либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или другими федеральными законами;

- в случае невозможности устранения допущенных при обработке персональных данных ошибок и/или на основании соответствующего предписания уполномоченного органа по защите прав субъектов персональных данных.

⁷ Ст. 21 ч. 3 Закон о персональных данных

⁸ Ст. 21 ч. 4 Закон о персональных данных

⁹ Ст. 21 ч. 4 Закон о персональных данных

¹⁰ Ст. 21 ч. 5 Закон о персональных данных

4.2.7.2 Персональные данные подлежат уничтожению (или обезличиванию) в срок, не превышающий десяти рабочих дней¹¹ с даты выявления неправомерной обработки персональных данных:

- 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 их 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 в иных случаях инициирует Ответственный за организацию обработки персональных данных.

4.2.7.5 Владелец процесса, в котором обрабатываются персональные данные, согласовывает уничтожение персональных данных путем направления служебной записки Ответственному за организацию обработки персональных данных.

4.2.7.6 Ответственный за организацию обработки персональных данных на основании информации, указанной в Перечне персональных данных, обрабатываемых в Учреждении, определяет, в каких еще процессах и в каких информационных системах персональных данных осуществляется обработка соответствующих персональных данных, которые необходимо уничтожить, и инициирует их уничтожение.

4.2.7.7 Ответственное за уничтожение персональных данных лицо назначается Ответственным за организацию обработки персональных данных из числа подчиненных ему работников. В случае с бумажными носителями персональных данных лицом, ответственным за уничтожение персональных данных, является 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 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 оно передает акт об уничтожении персональных данных Ответственному за организацию обработки персональных данных на подписание.

4.2.7.9 Ответственный за организацию обработки персональных данных подписывает акт об уничтожении персональных данных и готовит проект уведомления Учреждением субъекту персональных данных или его представителю об уничтожении персональных данных. После подписания руководством Учреждения он обеспечивает отправку уведомления адресату.

¹¹ Ст. 21 ч. 3 Закон о персональных данных

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 готовит проект уведомления об уничтожении персональных данных субъекту персональных данных или его представителю, а также в указанный орган, и после подписания руководством Учреждения обеспечивает их отправку адресатам.

4.2.7.11 В случае отсутствия возможности уничтожения персональных данных в течение установленных сроков персональные данные должны быть заблокированы, после чего – 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 Учреждения или с привлечением специализированной организации путем измельчения, сжигания или преобразования в целлюлозную массу таким образом, чтобы гарантировать невозможность их восстановления, а также иным способом.

4.2.7.14 Уничтожение персональных данных собственными силами должно оформляться актом об уничтожении персональных данных, с привлечением специализированной организации – актом по форме, предусмотренной договором.

4.2.7.15 Акт об уничтожении персональных данных должен содержать следующие обязательные сведения:

- дата и место уничтожения персональных данных;
- перечень персональных данных, подлежащих уничтожению, и отметка об уничтожении каждого из них либо их общего количества;
- способ уничтожения персональных данных;
- сведения о лице, присутствующем при уничтожении персональных данных, с указанием должности, фамилии и инициалов.

4.2.7.16 Акт об уничтожении персональных данных подписывается лицом, производившим уничтожение персональных данных, и Ответственным за организацию обработки персональных данных.

4.3 Обеспечение конфиденциальности персональных данных

4.3.1 Учреждение и иные лица, обладающие правом доступа к персональным данным (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 неправомерных действий выполняются следующие организационные меры:

- повышение осведомленности работников Учреждения 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 должны ознакомиться 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 Учреждения в зависимости от занимаемой ими должности.

4.3.3 Учреждение передает персональные данные на обработку третьим лицам (принимающей стороне), только если это необходимо для достижения целей обработки персональных данных, причем существенным условием передачи 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 персональными данными на автоматизированных рабочих местах

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

- принятые в Учреждении правила парольной политики;
- исключение возможности подсматривания информации на мониторе посторонними лицами, в том числе и с помощью технических средств (стационарных и встроженных 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 вносятся персональные данные, включается следующая информация:

– цель обработки персональных данных, наименование и адрес Учреждения, источник получения персональных данных, срок обработки персональных данных, перечень действий с персональными данными, 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 Учреждения.

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 Учреждении 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 Учреждения запираются.

5 Взаимодействие с государственными органами

5.1 Учреждение обязано уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением предусмотренных Порядком взаимодействия с уполномоченным органом по защите прав субъектов персональных данных случаев.

5.2 Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней¹² 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. Учреждение сообщает в указанный орган об устранении нарушений либо об уничтожении персональных данных в случае невозможности устранения нарушений в срок, не превышающий десяти рабочих дней¹³.

5.4 В установленных федеральным законодательством случаях Учреждение 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 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 Закон о персональных данных

¹³ Ст. 22 ч. 7 Закон о персональных данных

6 Правила доступа к персональным данным

6.1 В Учреждении 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 Учреждения предоставляется доступ к работе с персональными данными исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

6.3 Работники Учреждения, 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 Учреждения по представлению Ответственного за организацию обработки 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 Учреждения по согласованию с Ответственным за организацию обработки персональных данных путем подачи заявки на доступ с указанием цели и срока доступа и категорий персональных данных, к которым запрашивается доступ.

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

6.7 Предоставление и прекращение доступа пользователей к персональным данным осуществляется ответственными за эксплуатацию соответствующих информационных систем персональных данных¹⁴.

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

7 Требования к работникам, допущенным к обработке персональных данных

7.1 Все работники Учреждения, которым стали известны персональные данные, обрабатываемые в информационных системах персональных данных Учреждения, должны обеспечивать их конфиденциальность.

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

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

7.4 В Учреждении 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 Учреждения, 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 Учреждения несут ответственность в соответствии с разделом 8 настоящего Положения.

8 Ответственность за нарушения при обработке персональных данных

8.1 Работники Учреждения 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 Учреждения 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 персональным данным, раскрытия персональных данных и нанесения Учреждению, его работникам, клиентам, посетителям и другим субъектам персональных данных материального или иного ущерба виновные лица несут предусмотренную законодательством Российской Федерации ответственность.