



Комитет культуры и молодежной политики
администрации города Ставрополя
Ставропольского края

ПРИКАЗ

«17» сентября 2021 г.

г. Ставрополь

№ 204-02

Об организации работы и проведение работ по обработке и защиты персональных данных в комитете культуры и молодежной политике администрации города Ставрополя

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и во исполнение постановления Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»:

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Порядок организации и проведение работ по обработке и защиты персональных данных в комитете культуры и молодежной политике администрации города Ставрополя согласно приложения.

2. Контроль за исполнением настоящего приказа оставляю за собой.

3. Настоящий приказ вступает в силу со дня его подписания.

Руководитель комитета культуры
и молодежной политики
администрации города Ставрополя



Н.П. Головин

УТВЕРЖДЕН

приказом руководителя
комитета культуры
и молодежной политики
администрации города
Ставрополя

от 17.09.2021 № 204-ОД

ПОРЯДОК организации и проведение работ по обработке и защиты персональных данных в комитете культуры и молодежной политики администрации города Ставрополя

I. Общие положения

1. Настоящий Порядок организации и проведение работ по обработке и защиты персональных данных в комитете культуры и молодежной политики администрации города Ставрополя (далее соответственно – Порядок, комитет) определяет политику и условия обработки персональных данных, т.е. любых действий (операций) или совокупности действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных в комитете с использованием средств автоматизации и без использования таких средств.

2. Настоящий Порядок определяет правовые, организационные и технические меры необходимые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Во всех случаях, не урегулированных настоящим Порядком или другими нормативными документами комитета, необходимо руководствоваться действующим законодательством Российской Федерации.

4. Целью настоящего Порядка является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

5. Настоящий Порядок разработан в соответствии со следующими нормативными правовыми актами:

- Конституция Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;

Уголовный кодекс Российской Федерации;
Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 г № 687;

требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденное Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119;

Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

6. В целях реализации настоящего Порядка применяются следующие понятия и термины:

субъект – гражданин, обратившийся с обращением (жалобой или заявлением), гражданин, состоящий в договорных отношениях с комитетом, иное лицо, связанные с исполнением комитетом муниципальных задач и функций, определенных Положением о комитете культуры и молодежной политики администрации города Ставрополя, утвержденного постановлением администрации города Ставрополя от 02.02 2016 № 207;

субъект комитета – сотрудник комитета, бывший сотрудник комитета, близкие родственники сотрудника (супруг (а), дети, родители комитета, лица, претендующие на замещение должностей муниципальной службы, лица, замещающие должности руководителей муниципальных учреждений подведомственных комитету, лица, претендующие на замещение должностей руководителей муниципальных учреждений, подведомственных комитету);

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

актуальные угрозы безопасности персональных данных – совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом, которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

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

обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

персональные данные – любая информация, относящаяся к прямо или косвенно определенному субъекту или субъекту комитета;

предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

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

уполномоченный орган по защите прав субъектов, субъектов комитета – это федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

7. Настоящий Порядок являются обязательными для исполнения всеми сотрудниками комитета, имеющими доступ к персональным данным.

II. Цели и принципы обработки персональных данных

8. Комитет обрабатывает персональные данные субъектов, субъектов комитета, исключительно в следующих целях:

рассмотрение жалоб (обращений) субъектов;

осуществление гражданско-правовых отношений;

выполнение функций и задач, возложенных на комитет

о комитете культуры и молодежной политики администрации города
утвержденного постановлением администрации города Ставрополя
02.02 2016 № 207;

Положением
Ставрополя,
от

регулирование трудовых отношений и иных непосредственно связанных с ними отношений субъектов комитета.

9. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных целей в соответствии с пунктом 8 настоящего Порядка.

10. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных в соответствии с пунктом 8 настоящего Порядка.

11. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

12. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

13. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

14. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

15. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, субъект комитета.

16. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательными актами Российской Федерации.

III. Состав персональных данных

17. В целях ведения кадрового и бухгалтерского учета в комитете обрабатываются следующие персональные данные субъектов:

ФИО;

паспортные данные;

дата и место рождения;

данные о регистрации;

номер телефона (домашний, сотовый);

семейное положение;

сведения об образовании, квалификации;

сведения о наградах;

данные об изменении должностного положения, должность.

18. В целях обработки персональных данных субъектов в комитете обрабатываются следующие персональные данные:

фамилия, имя, отчество (ФИО);

паспортные данные;

дата и место рождения;

данные о регистрации;

данные о семье, семейном положении;

номер телефона, адрес email;

ИНН;

СНИЛС;

социальный статус;
финансовые данные;
данные военного билета;
категории льготности;
данные о количестве и датах предоставления социальных услуг.
Источниками персональных данных являются:
паспорт;
трудовая книжка;
свидетельство СНИЛС, ИНН;
документ об образовании;
военный билет.

IV. Порядок обработки персональных данных

19. Обработка и распространение персональных данных субъектов, субъектов комитета осуществляется с их письменного согласия, согласно приложения 1.

20. Опубликование и распространение персональных данных субъектов, субъектов комитета допускается в случаях, установленных законодательными актами Российской Федерации.

21. Субъект, субъект комитета принимает решение о предоставлении персональных данных и дает согласие на обработку его персональных данных и распространение персональных данных свободно, своей волей и в своем интересе.

22. Согласия на обработку и распространение персональных данных может быть дано субъектом, субъектом комитета или их представителями в соответствии с пунктом 19 настоящего Порядка.

23. Согласие на обработку и распространение персональных данных субъекта, субъектов комитета может быть отозвано субъектом, субъектом комитета в соответствии с положением статьи 9 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

24. В случае отзыва субъектом, субъектом комитета персональных данных согласия на обработку и (или) распространение персональных данных комитет вправе продолжить обработку персональных данных без согласия субъекта, субъекта комитета при наличии законных оснований.

25. В случае признания недееспособности субъекта, субъекта комитета согласие на обработку его персональных данных дает письменно законный представитель субъекта или субъекта комитета.

26. В случае смерти субъекта, субъекта комитета согласие на обработку его персональных данных дают наследники субъекта, субъекта комитета, если такое согласие не было дано субъектом, субъектом комитета при его жизни.

27. Субъект, субъект комитета обязан предоставлять комитету достоверные сведения о себе для обработки персональных данных.

28. Если персональные данные субъекта, субъекта комитета получены из общедоступных источников, то сроки их хранения не ограничиваются.

29. Обработка персональных данных осуществляется допущенными к обработке сотрудниками комитета, определенными приказом руководителя

комитета, которые действуют на основании инструкций, предусматривающих выполнение комплекса мероприятий по обеспечению безопасности персональных данных.

V. Особенности обработки персональных данных без использования средств автоматизации

30. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённого постановлением Правительства Российской Федерации от 15.09.2008 № 687.

31. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на комитет полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

типсовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, адрес комитета, фамилию, имя, отчество и адрес субъекта, субъекта комитета, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

типсовая форма должна предусматривать поле, в котором субъект, субъект комитета может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;

типсовая форма должна быть составлена таким образом, чтобы каждый из субъектов, субъектов комитета, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными, не имел возможности доступа к персональным данным иных лиц, содержащихся в указанной типовой форме и не нарушали прав и законных интересов иных лиц;

типсовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

32. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, а также если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными, должны быть приняты меры по обеспечению отдельной 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.

33. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

34. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

VI. Порядок уничтожения персональных данных

35. Уничтожение обработанных персональных данных в комитете в целях исключения их в дальнейшей обработке осуществляется в сроки, установленные законодательными актами Российской Федерации.

36. Персональные данные уничтожаются или обеспечивается их уничтожение в случае:

если получен отзыв от субъекта или субъекта комитета в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект, субъект комитета, иным соглашением между комитетом и субъектом или субъектом комитета;

если комитет не вправе осуществлять обработку персональных данных без согласия субъекта, субъекта комитета на основаниях, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими законодательными актами Российской Федерации;

если представлены субъектом, субъектом комитета или его представителем сведения, подтверждающие, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, в срок, не превышающий семи рабочих дней со дня предоставления субъектом, субъектом комитета или его представителем сведений;

если обеспечить правомерность обработки персональных данных невозможно, в срок, не превышающий десяти рабочих дней с даты выявления неправомерной

обработки персональных данных.

37. В случае отсутствия возможности уничтожения персональных данных в течение срока, осуществляется блокирование персональных данных или обеспечивается их блокирование и обеспечивается уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен законодательными актами Российской Федерации.

38. Об устранении допущенных нарушений или об уничтожении персональных данных комитет уведомляет субъект, субъекта комитета. Форма уведомления об уничтожении, (изменении, прекращении обработки, устранении нарушений персональных данных) приведена в приложении 2.

В случае, запроса об устранении допущенных нарушений или об уничтожении персональных данных уполномоченного органа по защите прав субъекта, субъекта комитета, комитет уведомляет дополнительно о проделанной работе орган по защите прав субъекта, субъект комитета.

39. Уничтожение персональных данных в комитете происходит штатными средствами комитета.

40. Уничтожение бумажных носителей персональных данных происходит путём измельчения на бумагорезательной машине, либо сжигания.

41. Уничтожение персональных данных осуществляет комиссия в составе членов комиссии и председателя, утвержденная приказом руководителя комитета.

42. Порядок уничтожения должен быть регламентирован в нормативных документах комитета.

43. Контроль за выполнением процедур уничтожения персональных данных осуществляет Ответственный за обеспечение безопасности и обработку персональных данных, назначенный приказом руководителя комитета.

44. После проведенного уничтожения должен быть подготовлен акт об уничтожении персональных данных. Форма акта приведена в приложении 3.

VII. Трансграничная передача персональных данных

45. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

46. Комитет не осуществляет трансграничную передачу персональных данных.

VIII. Права субъекта персональных данных

47. Субъект, субъект комитета имеет право на получение сведений, об обработке его персональных данных, за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», в том числе содержащей:

подтверждение факта обработки персональных данных;

правовые основания и цели обработки персональных данных;

цели и применяемые способы обработки персональных данных;
наименование и место нахождения комитета, сведения о лицах (за исключением сотрудников комитета), которые имеют доступ к персональным данным;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту, субъекту комитета, источник их получения;

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

порядок осуществления субъектом, субъектом комитета прав, предусмотренных Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

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

иные сведения, предусмотренные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» или другими законодательными актами Российской Федерации.

48. Сведения, об обработке персональных данных, предоставляются субъекту, субъекту комитета в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам, субъектам комитета.

49. Сведения, об обработке персональных данных, предоставляются субъекту, субъекту комитета персональных данных или его представителю комитетом при обращении либо при получении письменного запроса субъекта, субъекта комитета или их представителей.

50. Субъект, субъект комитета вправе требовать уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

51. Субъект, субъект комитета вправе обратиться повторно письменно в комитет или направить повторный запрос в целях получения сведений об обработке его персональных данных, а также в целях ознакомления с обрабатываемыми персональными данными, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

52. Субъект, субъект комитета вправе требовать от комитета разъяснения о порядке принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, а также, заявить возражение против такого решения.

53. Если субъект, субъект комитета считает, что комитет осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект, субъект комитета вправе обжаловать действия или бездействие комитета в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

54. Субъект, субъект комитета имеет право на защиту своих прав и законных

интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

IX. Права комитета

55. Комитет вправе отказать субъекту, субъекту комитета в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

X. Обязанности комитета

56. Комитет обязан уведомить субъект, субъект комитета об их персональных данных, находящихся в комитете, обеспечить свободный доступ к их персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных действующим законодательством. Форма уведомления о персональных данных, содержащихся в комитете приведена в приложении 4.

57. Комитет обязан разъяснить субъекту, субъекту комитета порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом, субъектом комитета своих прав и законных интересов.

58. Комитет обязан рассмотреть возражение субъекта, субъекта комитета против принятия решения на основании исключительно автоматизированной обработки их персональных данных, в течение тридцати дней со дня его получения и уведомить субъекта, субъекта комитета о результатах рассмотрения такого возражения.

59. Комитет обязан предоставить субъекту или субъекту комитета по их просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

60. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте, субъекте комитета или персональных данных субъекта, субъекта комитета или их представителей при их обращении либо при получении запроса субъекта, субъекта комитета или их представителей комитет дает в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного законодательного акта Российской Федерации, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта, субъекта комитета или его представителя либо с даты получения запроса субъекта, субъекта комитета или их представителей.

61. В срок, не превышающий семи рабочих дней со дня предоставления субъектом, субъектом комитета или его представителем сведений, подтверждающих,

что персональные данные являются неполными, неточными или неактуальными, комитет обязан внести в них необходимые изменения.

62. В срок, не превышающий семи рабочих дней со дня представления субъектом, субъектом комитета или их представителями сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, комитет обязан уничтожить такие персональные данные субъекта, субъекта комитета.

63. Комитет обязан уведомить субъекта, субъекта комитета или их представителей о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта, субъекта комитета были переданы.

64. Если предоставление персональных данных является обязательным в соответствии с законодательством Российской Федерации, комитет обязан разъяснить субъекту, субъекту комитета юридические последствия отказа предоставить их персональные данные.

65. Если персональные данные получены не от субъекта, субъекта комитета, комитет, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить субъекту, субъекту комитета следующую информацию, согласно приложения 5:

- 1) наименование либо фамилия, имя, отчество и адрес учреждения или его представителя;
- 2) цель обработки персональных данных и ее правовое основание;
- 3) предполагаемые пользователи персональных данных;
- 4) установленные Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» права субъекта, субъекта комитета;
- 5) источник получения персональных данных.

66. Комитет обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

66. Блокирование персональных данных субъекта персональных данных осуществляется или обеспечивается в случае:

выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки;

выявления неточных персональных данных при обращении субъекта, субъекта комитета либо по запросу уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения.

67. В случае подтверждения факта неточности персональных данных комитет обязан блокировать персональные данные либо обеспечить их уточнение в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

68. Обработка персональных данных прекращается в случае:

выявления неправомерной обработки персональных данных, в срок, не превышающий трех рабочих дней с даты этого выявления;
достижения цели обработки персональных данных;
отзыва субъектом, субъектом комитета согласия на обработку их персональных данных.

69. Комитет обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

XI. Передача персональных данных третьим лицам

709. Комитет получивший доступ к персональным данным, обязан не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта, субъекта комитета, если иное не предусмотрено законодательством Российской Федерации.

71. Передача персональных данных субъектов, субъектов комитета не допускается без письменного согласия, за исключением случаев, установленных законодательством Российской Федерации, согласно приложения б.

72. Персональные данные субъектов, субъектов комитета передаются в следующие государственные и муниципальные структуры:

Федеральная налоговая служба;

Фонд социального страхования Российской Федерации;

Пенсионный фонд Российской Федерации;

администрация города Ставрополя;

министерство культуры Ставропольского края.

73. Не допускается передача персональных данных по открытым каналам связи, в том числе по телефону.

74. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и/или путем применения программных и технических средств.

XII. Меры по защите персональных данных

75. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности комитета.

76. Комитет при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

77. Мероприятия по защите персональных данных определяются настоящим Порядком, приказами, инструкциями и другими внутренними документами комитета. Форма расписки об ознакомлении субъекта, субъекта комитета с «Положением о порядке организации и проведении работ по обработке и защите персональных данных комитета культуры и молодежной политики администрации города Ставрополя» уведомления о персональных данных содержащихся в комитете приведена в приложении 7.

78. Для защиты персональных данных в комитете применяются следующие меры:

назначение ответственного за обеспечение безопасности и обработку персональных данных;

назначение администратора информационной безопасности информационных систем персональных данных;

назначение администратора информационных систем персональных данных;

издание, документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

осуществление внутреннего контроля и аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике комитета в отношении обработки персональных данных, локальным актам комитета;

оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых комитетом мер;

ознакомление сотрудников комитета, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику комитета в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных сотрудников;

определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных;

применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

учет машинных носителей персональных данных;

обнаружение фактов несанкционированного доступа к персональным данным

и принятием мер;

восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

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

контроль за принимаемыми мерами по обеспечению безопасности персональных данных;

ограничение и регламентация состава сотрудников комитета, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

распределение персональной ответственности между сотрудниками комитета, участвующими в обработке персональных данных, за выполнение требований по обеспечению безопасности персональных данных;

исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка персональных данных и находится соответствующая вычислительная техника;

организация порядка уничтожения персональных данных;

оборудование помещений, в которых обрабатываются и хранятся персональные данные субъектов, субъектов комитета, замками;

регулярные инструктажи сотрудников по вопросам, связанным с обеспечением безопасности персональных данных;

закрытие помещений, в которых обрабатываются и хранятся персональные данные субъектов, субъектов комитета, в рабочее время при отсутствии в них сотрудников;

проведение уборки помещений, в которых хранятся персональные данные, производиться в присутствии соответствующих сотрудников;

запрещение самостоятельного подключения средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет;

резервирование персональных данных (создание резервных копий).

ХIII. Допуск сотрудников к обработке персональных данных

79. При допуске к обработке персональных данных необходимо руководствоваться приказом руководителя комитета о допуске сотрудников комитета города Ставрополя к обработке персональных данных.

80. Доступ конкретных лиц к персональным данным в информационной системе персональных данных осуществляется на основании служебных записок (заявок). Служебные записки на доступ учитываются и хранятся администратором информационной безопасности информационных систем персональных данных.

81. Конкретный регламент предоставления доступа определен в «Инструкции

по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационной системы персональных данных комитета».

XIV. Обучение персонала, участвующего в обработке персональных данных

82. Должно проводиться регулярное обучение сотрудников комитета по вопросам, связанным с обеспечением безопасности персональных данных.

83. Определены следующие форматы обучения:

полные курсы (длительностью 5 дней и более);

кратковременные курсы (длительностью от 1 до 3 дней);

внешние и внутренние семинары;

конференции;

инструктажи.

84. Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий сотрудников:

ответственный за обеспечение безопасности и обработку персональных данных;

администратор информационной безопасности информационных систем персональных данных.

85. Для обучения остальных категорий персонала, участвующих в процессах обработки персональных данных, должны проводиться:

внутренние семинары;

инструктажи.

86. Внутренние семинары проводятся ответственным за обеспечение безопасности и обработку персональных данных, администратором информационной безопасности информационных систем персональных данных, а также приглашенными специалистами или другими подготовленными лицами.

87. Обучение каждой категории сотрудников комитета должно проводиться не реже одного раза в год.

88. Инструктажи проводятся в отношении отдельных лиц, по мере необходимости администратором информационной безопасности информационных систем персональных данных комитета, ответственным за обеспечение безопасности и обработку персональных данных в комитете.

89. При необходимости могут разрабатываться инструкции, описывающие особенности обработки персональных данных в каждой информационной безопасности информационных систем персональных данных для отдельных категорий (групп) сотрудников комитета.

90. Проведения инструктажей должно фиксироваться в «Журнале учета проведения инструктажей по вопросам защиты информации».

XV. Защита от несанкционированного физического доступа к элементам информационных систем персональных данных

91. Мероприятия по физическому контролю доступа включают:

контроль доступа на территорию;
контроль доступа в помещения с оборудованием информационных систем персональных данных;

контроль доступа к техническим средствам информационных систем персональных данных;

контроль перемещений физических компонентов информационных систем персональных данных;

92. Помещения с серверным, телекоммуникационным и сетевым оборудованием информационных систем персональных данных должны иметь входные двери с замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников комитета, отвечающих за обслуживание данного оборудования.

93. Нахождение в помещении лиц, не участвующих в технологических процессах обработки персональных данных (обслуживающий персонал комитета, другие сотрудники комитета), должно допускаться только в присутствии сотрудников комитета, работающих с информационными системами персональных данных.

94. Расположение вычислительной техники должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями информационных систем персональных данных.

95. Помещения, в которых ведется обработка персональных данных, в нерабочее время, а также в случаях отсутствия в рабочее время работников, имеющих право доступа в помещения, должны закрываться на ключ.

96. Передача технических средств в ремонт, их замена или списание проводится только после полного удаления персональных данных со встроенных накопителей информации накопителей на жестких магнитных дисках в помещениях, в которых ведется обработка персональных данных.

97. Ответственность за доступ в помещение, в котором ведется обработка персональных данных, возлагается на работников, имеющих право доступа в помещение.

XVI. Резервирование персональных данных

98. Резервирование персональных данных должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

99. Резервированию должна подвергаться информация на серверах с информационными системами персональных данных.

100. Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

101. Хранение резервных копий должно осуществляться в сейфах (запираемых шкафах, ящиках). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

102. Доступ к резервным копиям должен быть строго регламентирован.

103. Резервирование должно осуществляться в соответствии с инструкцией

резервного копирования комитета.

XVII. Реагирование на нештатные ситуации

104. Для эффективного реагирования на нештатные ситуации, возникающие при обработке персональных данных, в комитете должны быть регламентированы следующие вопросы:

порядок определения нештатной ситуации;

порядок оповещения сотрудников при возникновении различных нештатных ситуаций;

порядок действий персонала в нештатных ситуациях.

105. В комитете должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

106. В рамках данного процесса должны решаться следующие задачи:

расследование инцидентов, связанных с безопасностью персональных данных;

ликвидация последствий инцидентов связанных с безопасностью персональных данных;

принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

107. Реагирование на нештатные ситуации должно производиться в соответствии с «Инструкцией по действиям пользователей персональных данных в нештатных ситуациях».

XVIII. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

108. Ответственность за организацию работы с персональными данными субъектов, субъектов комитета возлагается на руководителя комитета.

109. Сотрудники комитета, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, субъекта комитета несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательными актами Российской Федерации.

110. Каждый сотрудник комитета, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации. Форма обязательства о неразглашении персональных данных содержащихся в комитете приведена в приложении 8.

XIX. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

111. Внутренний контроль соответствия обработки персональных данных в комитете требованиям к защите персональных данных направлен на выявление и предотвращение нарушений требований законодательства Российской Федерации

в области персональных данных и осуществляется путем проведения проверок условий обработки персональных данных и соответствия обработки персональных данных требованиям, установленным законодательством Российской Федерации в области персональных данных и принятыми в соответствии с ними нормативными правовыми актами комитета (далее соответственно – внутренний контроль, проверки соответствия обработки персональных данных установленным требованиям).

112. Проведение проверок соответствия обработки персональных данных установленным требованиям организуется ответственным лицом на основании ежегодного плана осуществления внутреннего контроля, утверждаемого руководителем комитета.

Проведение внеплановых проверок соответствия обработки персональных данных установленным требованиям организуется ответственным лицом на основании поступившего в комитет письменного заявления субъекта, субъекта комитета о нарушениях правил обработки персональных данных в течение 3 рабочих дней со дня поступления соответствующего заявления.

113. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает соответствие установленным уровням защищенности персональных данных;

2) порядок и условия применения средств защиты информации;

3) оценка эффективности принимаемых мер по обеспечению безопасности персональных данных в информационных системах комитета;

4) состояние учета машинных носителей персональных данных;

5) соблюдение правил доступа к персональным данным;

6) наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер их защиты, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы комитета и по реагированию на компьютерные инциденты в них;

7) выполнение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) выполнение мероприятий по обеспечению целостности персональных данных.

114. Проверка соответствия обработки персональных данных установленным требованиям должна быть завершена в течение месяца со дня принятия решения о ее проведении.

115. Результаты проведения проверки соответствия обработки персональных данных установленным требованиям в виде Акта внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – акт внутреннего контроля) доводится ответственным лицом до сведения

руководителя комитета.

116. Акт внутреннего контроля должен содержать одно из следующих заключений:

1) в деятельности комитета отсутствуют нарушения требований законодательства Российской Федерации в области персональных данных;

2) в деятельности комитета выявлены нарушения требований законодательства Российской Федерации в области персональных данных. В этом случае в заключении также указываются: характер выявленных нарушений требований законодательства Российской Федерации в области персональных данных (с указанием конкретных статей и (или) пунктов нормативных правовых актов Российской Федерации, требования которых были нарушены); лица, допустившие данные нарушения; предложения по пресечению и предупреждению нарушений требований законодательства Российской Федерации в области персональных данных.

На основании представленного доклада по результатам проверки руководитель комитета принимает соответствующее решение.