УТВЕРЖДАЮ
Директор МКУ КМЦИКТ «Старт»
_____ Дьяченко В.А.
«02» _____ 2019 г.

ПОЛОЖЕНИЕ

об обработке персональных данных в муниципальном казённом учреждении муниципального образования город Краснодар «Краснодарский методический центр информационно-коммуникационных технологий «Старт»

Раздел I Термины и определения

1. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
2. Неавтоматизированная обработка персональных данных - обработка персональных данных осуществляются при непосредственном участии человека.
3. 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.
4. Биометрические персональные данные - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных.
5. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
6. Информационная система персональных данных (далее - ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
7. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
8. 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.

9. Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

10. Персональные данные - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

11. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определённому кругу лиц.

12. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

13. Специальные категории персональных данных - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни.

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

15. 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.

16. 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.

Раздел II
Общие положения

17. Целью настоящего Положения 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.

18. Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информа-

ционных технологиях и о защите информации»;

- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687;

- Постановление Правительства Российской Федерации от 06.06.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

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

- Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;

- Конституция Российской Федерации;

- Трудовой кодекс Российской Федерации;

- Гражданский кодекс Российской Федерации;

- Налоговый кодекс Российской Федерации;

- Уголовный кодекс Российской Федерации;

- нормативные и методические документы ФСБ России, ФСТЭК России, Роскомнадзора.

19. Настоящее Положение определяет порядок 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 муниципальном казённом учреждении муниципального образования город Краснодар «Краснодарский методический центр информационно-коммуникационных технологий «Старт» (далее — учреждение).

20. Настоящее Положение 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.

21. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В поручении учреждения должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны

быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

22. Во всех случаях, не урегулированных настоящим Положением или другими нормативными документами учреждения, необходимо руководствоваться действующим законодательством Российской Федерации.

23. Настоящее Положение вступает в силу с момента его утверждения и действует до замены его новым Положением.

24. Все изменения в Положение вносятся приказом директора учреждения.

25. Настоящее Положение и изменения к нему являются обязательными для исполнения всеми сотрудниками, имеющими доступ к персональным данным.

Раздел III
Принципы обработки персональных данных

26. Обработка персональных данных должна осуществляться на законной и справедливой основе.

27. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определённых и законных целей.

28. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

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

30. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

31. Содержание и объём обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

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

33. 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.

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

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

Раздел IV
Порядок обработки персональных данных

36. Обработка персональных данных субъектов персональных данных учреждения осуществляется с их письменного согласия, которое действует со дня их поступления на работу.

37. Опубликование и распространение персональных данных субъектов учреждения допускается в случаях, установленных законодательством Российской Федерации.

38. Субъект персональных данных принимает решение о предоставлении персональных данных и даёт согласие на их обработку свободно, своей волей и в своём интересе.

39. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем.

40. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с положением статьи 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

41. В случае отзыва субъектом персональных данных согласия на обработку персональных данных учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии законных оснований.

42. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.

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

44. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, осуществляется с согласия в письменной форме (Приложение № 5) субъекта персональных данных на трансграничную передачу его персональных данных.

45. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

46. Субъект персональных данных обязан предоставлять учреждению достоверные сведения о себе.

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

48. Обработка персональных данных осуществляется допущенными к обработке сотрудниками учреждения, определёнными приказом директора

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

Раздел V
Особенности обработки персональных данных без использования средств автоматизации

49. 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.

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

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

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

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, 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;

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

51. 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 раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определённых

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.

52. 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 (удаление, вымарывание).

53. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путём 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 путём изготовления нового материального носителя с уточнёнными персональными данными.

54. При составлении типовых форм необходимо, чтобы каждый субъект персональных данных, чьи персональные данные указаны в документе, имел возможность ознакомиться со своими персональными данными, содержащими в документе, не нарушая прав и законных интересов иных лиц.

Раздел VI
Порядок уничтожения персональных данных

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

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

- если получен отзыв от субъекта персональных данных 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 персональных данных, иным соглашением между учреждением и субъектом персональных данных;

- если учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами;

- если достигнуты цели обработки персональных данных, в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между учреждением и субъектом персональных данных;

- если представлены субъектом персональных данных 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 персональных данных 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.

57. 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 федеральными законами.

58. Об устранении допущенных нарушений или об уничтожении персональных данных учреждение уведомляет субъект персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

59. Уничтожение персональных данных в ИСПДн учреждения происходит штатными средствами учреждения, либо за счёт обезличивания персональных данных.

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

61. Уничтожение персональных данных осуществляет комиссия в составе членов комиссии и председателя.

62. Порядок уничтожения персональных данных должен быть регламентирован в нормативных документах учреждения.

63. Контроль за выполнением процедур уничтожения персональных данных осуществляет Ответственный за обеспечение безопасности и обработку персональных данных.

64. После проведенного уничтожения должен быть подготовлен акт об уничтожении персональных данных. Форма акта приведена в Приложении № 1.

Раздел VII
Трансграничная передача персональных данных

65. 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 № 152-ФЗ «О персональных данных».

66. Учреждение не осуществляет трансграничную передачу персональных данных.

Раздел VIII
Цель обработки персональных данных

67. К субъектам персональных данных в учреждении относятся:
- сотрудники;
- кандидаты на замещение вакантных должностей;
- граждане.

68. Целью обработки персональных данных является:
- ведение кадрового и бухгалтерского учёта сотрудников;
- оказание муниципальных услуг.

Раздел IX
Состав персональных данных

69. В целях ведения кадрового и бухгалтерского учёта в учреждении обрабатываются следующие персональные данные сотрудников:
- Ф.И.О.;
- дата и место рождения;
- паспортные данные;
- гражданство;
- данные о регистрации;
- номер телефона (домашний, сотовый);
- семейное положение;
- сведения об образовании, квалификации;
- сведения о доходе;
- сведения о воинском учёте;
- данные об изменении должностного положения, должность;
- ИНН, СНИЛС;
- номер счёта в банке;
- адрес проживания;
- водительское удостоверение;
- данные медицинской справки о допуске к управлению транспортным средством.

70. В целях обработки запросов граждан в учреждении обрабатываются следующие персональные данные граждан:

- Ф.И.О.;
- дата и место рождения;
- паспортные данные;
- гражданство;
- данные о регистрации;
- номер телефона (домашний, сотовый);
- сведения об образовании, квалификации;
- сведения о воинском учёте;
- данные места работы, должность;
- адрес проживания.

71. Источниками персональных данных являются:

- паспорт;
- трудовая книжка;
- свидетельство СНИЛС, ИНН;
- документ об образовании;
- военный билет;
- водительское удостоверение;
- медицинская справка о допуске к управлению транспортным средством.

Раздел X
Права субъекта персональных данных

72. Субъект персональных данных имеет право на получение информации, касающейся обработки его 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 учреждения, сведения о лицах (за исключением сотрудников), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с учреждением или на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка

поручена или будет поручена такому лицу;

- иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

73. Субъект персональных данных имеет право на получение сведений, об обработке его персональных данных, за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

75. Сведения, об обработке персональных данных, предоставляются субъекту персональных данных или его представителю учреждением при обращении либо при получении запроса субъекта персональных данных или его представителя.

76. Субъект персональных данных вправе обратиться повторно к учреждению или направить повторный запрос в целях получения сведений об обработке его персональных данных и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса.

77. Субъект персональных данных 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.

78. Субъект персональных данных вправе обратиться повторно к учреждению 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 объёме по результатам рассмотрения первоначального обращения.

79. Субъект персональных данных вправе требовать от учреждения 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.

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

81. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Раздел XI
Права оператора

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

Раздел XII
Обязанности оператора

83. Оператор обязан разъяснить субъекту персональных данных 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 персональных данных своих прав и законных интересов.

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

85. Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», за исключением случаев, предусмотренных частью 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

86. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Оператор даёт в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

87. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор обязан внести в них необходимые изменения.

88. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными

или не являются необходимыми для заявленной цели обработки, Оператор обязан уничтожить такие персональные данные.

89. Оператор обязан уведомить субъекта персональных данных или его представителя о внесённых изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

90. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

91. Если персональные данные получены не от субъекта персональных данных, Оператор, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию (Приложение № 9):

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и её правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» права субъекта персональных данных;
- источник получения персональных данных.

92. Оператор 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.

93. 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 персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных с момента такого обращения или получения указанного запроса на период проверки.

94. В случае подтверждения факта неточности персональных данных Оператор обязан обеспечить их уточнение в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

95. Обработка персональных данных прекращается или обеспечивается прекращение их обработки в случае:

- выявления неправомерной обработки персональных данных, в срок, не превышающий трёх рабочих дней с даты этого выявления;

- достижения цели обработки персональных данных;

- отзыва субъектом персональных данных согласия на обработку его персональных данных.

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

Раздел XIII
Передача персональных данных третьим лицам

97. Учреждение и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

98. Передача персональных данных сотрудников учреждения не допускается без письменного согласия, за исключением случаев, установленных федеральными законами.

99. Персональные данные сотрудников учреждения передаются в следующие государственные и негосударственные структуры:

- ОАО «УРАЛСИБ»;
- учреждение Федеральной налоговой службы;
- учреждение Федерального казначейства;
- Фонд социального страхования Российской Федерации;
- Центральный аппарат Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций;
- Пенсионный фонд Российской Федерации;
- Муниципальное казённое учреждение муниципального образования город Краснодар «Централизованная бухгалтерия департамента образования администрации муниципального образования город Краснодар»;
- Военные комиссариаты Российской Федерации.

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

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

Раздел XIV
Меры по защите персональных данных

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

процессе деятельности учреждения.

103. Учреждение 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.

104. Мероприятия по защите персональных данных определяются настоящим Положением, приказами, инструкциями и другими внутренними документами учреждения.

105. Для защиты персональных данных в учреждении применяются следующие меры:

- назначение ответственного за обеспечение безопасности и обработку персональных данных;
- назначение администратора ИСПДн;
- назначение администратора информационной безопасности ИСПДн;
- 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 согласно Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике учреждения в отношении обработки персональных данных, локальным актам учреждения;
- оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых учреждением мер;
- ознакомление сотрудников учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику учреждения 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;

- учёт 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 обеспечение регистрации и учёта 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, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;

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

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

- организация порядка уничтожения персональных данных;

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

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

- закрытие помещений, в которых обрабатываются и хранятся персональные данные субъектов персональных данных, 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).

Раздел XV
Допуск персонала к обработке ПДн

106. При допуске к обработке персональных данных необходимо руководствоваться Приказом о допуске сотрудников муниципального казённого учреждения муниципального образования город Краснодар «Краснодарский методический центр информационно-коммуникационных технологий «Старт» к обработке персональных данных.

107. Доступ конкретных лиц к персональным данным в ИСПДн осуществляется на основании служебных записок (заявок). Служебные записки на доступ учитываются и хранятся администратором информационной безопасности ИСПДн.

108. Конкретный регламент предоставления доступа определен в «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн».

Раздел XVI
Обучение персонала, участвующего в обработке ПДн

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

110. 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.

111. 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 ИСПДн.

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

- внутренние семинары;
- инструктажи.

113. Внутренние семинары проводятся ответственным за обеспечение безопасности и обработку персональных данных, администратором информационной безопасности ИСПДн, а также приглашёнными специалистами или другими подготовленными лицами. Все семинары следует проводить с использованием презентации.

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

115. Инструктажи проводятся в отношении отдельных лиц, по мере необходимости администратором информационной безопасности ИСПДн, ответственным за обеспечение безопасности и обработку персональных данных.

116. При необходимости могут разрабатываться инструкции, описывающие особенности обработки персональных данных в каждой ИСПДн, для отдельных категорий (групп) персонала.

117. Проведения инструктажей должно фиксироваться в «Журнале учёта проведения инструктажей по вопросам защиты информации».

Раздел XVII
Защита от несанкционированного физического доступа к элементам ИСПДн

118. Мероприятия по физическому контролю доступа включают:
- контроль доступа на территорию;
- контроль доступа в помещения с оборудованием ИСПДн;
- контроль доступа к техническим средствам ИСПДн;
- контроль перемещений физических компонентов ИСПДн.

119. Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надёжными замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников, отвечающих за обслуживание данного оборудования.

120. Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками.

121. Нахождение в помещении лиц, не участвующих в технологических процессах обработки персональных данных (обслуживающий персонал, другие сотрудники), должно допускаться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

122. Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями ИСПДн.

123. В нерабочее время, по окончании рабочего дня двери помещений должны быть закрыты на замок.

124. При выносе устройств, хранящих персональные данные, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

Раздел XVIII
Резервирование ПДн

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

126. Резервированию должна подвергаться информация на серверах ИСПДн.

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

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

129. Доступ к резервным копиям должен быть строго регламентирован.

130. Резервирование должно осуществляться в соответствии с инструкцией резервного копирования учреждения.

Раздел XVIII
Реагирование на нештатные ситуации

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

- порядок определения нештатной ситуации;
- порядок оповещения сотрудников при возникновении различных нештатных ситуаций;
- порядок действий персонала в нештатных ситуациях.

132. В учреждении должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

133. 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.

134. Реагирование на нештатные ситуации должно производиться в соответствии с «Инструкцией по действиям пользователей ИСПДн в нештатных ситуациях».

Раздел XIX
Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

135. Ответственность за контроль соблюдения требований по обработке персональных данных, контроль соблюдения прав и свобод субъектов персональных данных возлагается на директора учреждения.

136. Юридические и физические лица, в соответствии со своими полно-

мочиями обрабатывающие информацию о гражданах, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

137. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

138. Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несёт персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

139. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, содержащую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на сотрудников, не обладающих правом доступа к персональным данным.

ПРИЛОЖЕНИЕ № 1
к Положению об обработке персональных
данных МКУ КМЦИКТ «Старт»

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

работника

,

(Ф.И.О.)

Проживающий по адресу: _____

Паспорт № _____ , выданный _____

(кем и когда)

настоящим даю свое согласие на обработку в муниципальное казённое учреждение Краснодарский методический центр информационно-коммуникационных технологий «Старт», 350000, г.Краснодар, ул. им.Коммунаров, 119 (далее - МКУ КМЦИКТ «Старт») моих персональных данных, к которым относятся:

- паспортные данные;
- данные страхового Свидетельства государственного пенсионного страхования;
- данные документа воинского учета[1];
- документы об образовании, профессиональной переподготовке, повышении квалификации, стажировки, присвоении ученой степени, ученого звания (если таковые имеются);
- анкетные данные, предоставленные мною при поступлении на работу или в процессе работы (в том числе - автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);
- данные иных документов, которые с учетом специфики работы ив соответствии с законодательством Российской Федерации должны быть предъявлены мною при заключении трудового договора или в период его действия;
- данные трудового договора и соглашений к нему;
- данные кадровых приказов о моем приеме, переводах, увольнении;
- данные личной карточки по формам Т-2 и Т-1;
- данные документов о прохождении мной аттестации, собеседования, повышения квалификации. результатов оценки и обучения;
- фотография;
- иные сведения обо мне, которые необходимы МКУ КМЦИКТ «Старт» для корректного документального оформления правоотношений между мною и МКУ КМЦИКТ «Старт».

Я даю согласие на использование моих персональных данных в целях:

- корректного документального оформления трудовых правоотношений между мною и МКУ КМЦИКТ «Старт»;
- обеспечения выполнения мною должностных обязанностей;
- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренным действующим законодательством;
- предоставления информации в медицинские учреждения, страховые компании;
- обеспечения предоставления мне социального пакета.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу третьим лицам), обезличивание, блокирование, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными, предусмотренных действующим законодательством Российской Федерации.

МКУ КМЦИКТ «Старт» гарантирует, что обработка моих личных данных осуществляется в соответствии с действующим законодательством РФ и «Положением о защите персональных данных работников МКУ КМЦИКТ «Старт», с которым я ознакомлен (а) при трудоустройстве в МКУ КМЦИКТ «Старт».

Данное Согласие действует с момента заключения мною Трудового договора с МКУ КМЦИКТ «Старт» и до истечения сроков, установленных действующим законодательством Российской Федерации.

Я подтверждаю, что, давая такое Согласие, я действую своей волей и в своих интересах.

Дата: _____ Подпись _____/_____ /

ПРИЛОЖЕНИЕ № 2
к Положению об обработке персональных
данных МКУ КМЦИКТ «Старт»

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО

о неразглашении информации, содержащей персональные данные, обрабатываемый в муниципальном казённом учреждении Краснодарский методический центр информационно-коммуникационных технологий «Старт»

Я,_____

(фамилия, имя, отчество)

исполняющий (-ая) должностные обязанности _____

(должность)

_____

(наименование структурного подразделения)

предупрежден (-а) о том, что на период исполнения должностных обязанностей в соответствии с должностной инструкцией мне будет предоставлен допуск к информации, содержащей персональные данные, перечисленные в приказе «Об утверждении перечня персональных данных, обрабатываемых в МКУ КМЦИКТ «Старт» от «____»_____ 20____ г. №

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.

2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному руководителю.

3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.

4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.

5. После прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

6. Я предупрежден (-а) о том, что в случае нарушения данного обязательства буду привлечен (-а) к ответственности в соответствии с действующим законодательством Российской Федерации.

7. С Правилами обработки персональных данных ознакомлен (-а).

«_____»_____ 20____г. _____/_____

Подпись Расшифровка

ПРИЛОЖЕНИЕ № 3
к Положению об обработке персональных
данных МКУ КМЦИКТ «Старт»

ТИПОВАЯ ФОРМА РАЗЪЯСНЕНИЯ

юридических последствий отказа предоставить свои персональные данные

Мне,__
(фамилия, имя, отчество)

проживающий (-ая) по адресу _____
(адрес регистрации)

(документ, удостоверяющий личность, серия, номер, кем и когда выдан)

в соответствии с частью 2 статьи 18 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» разъяснены юридические последствия отказа предоставить свои персональные данные муниципальному казённому учреждению Краснодарский центр информационно-коммуникационных технологий «Старт» (далее - Центр «Старт»), зарегистрированному по адресу: 350000, г.Краснодар, ул. им.Коммунаров, д. 119.

В соответствии с приказом «Об утверждении перечня персональных данных, обрабатываемых в МКУ КМЦИКТ «Старт» от« _____» _____ 20__ г. №__ , определён перечень персональных данных, которые субъект персональных данных обязан предоставить уполномоченным лицам Центр «Старт» в связи с предоставлением услуг консультационного характера.

Я предупрежден (-а), что в случае отказа предоставить свои персональные данные уполномоченным лицам Центра «Старт» предоставление консультационных услуг не может быть выполнено в полном объеме.

«_____»_____ 20____г. _____/_____
Подпись Расшифровка