Утверждено
приказом исполняющего обязанности директора
ГКУ СК «Краевой центр информтехнологий»
№ 45-од от 08.04.2019г

ПОЛОЖЕНИЕ
о порядке обработки и защиты персональных данных в ГКУ СК «Краевой центр информтехнологий»

Содержание

1. Общие положения

1.1. Положение о порядке обработки и защиты персональных данных в ГКУ СК «Краевой центр информтехнологий» (далее – Положение) определяет порядок и условия обработки персональных данных (далее – ПДн) в ГКУ СК «Краевой центр информтехнологий» (далее – Оператор), включая порядок передачи ПДн третьим лицам, особенности автоматизированной и неавтоматизированной обработки ПДн, порядок доступа к ПДн, систему защиты ПДн, порядок организации внутреннего контроля и ответственности за нарушения при обработке ПДн, а также иные вопросы, связанные с ПДн.

1.2. К ПДн Оператора относятся:

- ПДн сотрудников Оператора;
- ПДн, обрабатываемые Оператором для выполнения заранее определенных законных целей.

1.3. Положение разработано в соответствии с законодательством Российской Федерации о ПДн и нормативными методическими документами исполнительных органов государственной власти по вопросам безопасности ПДн при их обработке в информационных системах ПДн (далее – ИСПДн).

1.4. Действие Положения распространяются на все процессы по сбору, систематизации, накоплению, хранению, уничтожению, использованию, распространению (в том числе передачу), обезличиванию, блокированию, уничтожению ПДн, осуществляемых с использованием средств автоматизации и без их использования.

1.5. Положение определяет необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к ПДн. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты ПДн.

1.6. Для целей Положения используются следующие основные понятия:

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

безопасность персональных данных – состояние защищенности ПДн, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в ИСПДн;

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

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

конфиденциальность персональных данных – обязательное для соблюдения Оператором или иным получившим доступ к ПДн лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам;

обработка персональных данных – любое действие (операция) или совокупность действий, 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 (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

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

оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

персональные данные – любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту ПДн);

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

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

технические средства информационных систем персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДН, а также иных несанкционированных действий при их обработке в ИСПДн;

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

1.7. Положение вступает в силу с момента его утверждения Оператором и действует бессрочно, до замены его новым Положением.

1.8. Все изменения в Положение вносятся приказом руководителя Оператора.

1.9. Сотрудники Оператора, допущенные к работе с ПДн на основании приказа руководителя Оператора, должны быть ознакомлены с настоящим Положением под роспись.

2. Цели и задачи обработки ПДн

2.1. Обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн. Содержание и объем, обрабатываемых ПДн должны соответствовать заявленным целям обработки таких данных.

2.2. Под обработкой ПДн понимаются действия (операции) с ПДн, включающие:

- сбор, хранение, уточнение (обновление, изменение);
- систематизацию, накопление;
- использование, распространение, передачу;
- обезличивание, блокирование, уничтожение.

2.3. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.4. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.5. Целями обработки ПДн являются:

- организация учета сотрудников для обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотруднику в трудоустройстве, обучении, пользования различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», а также законодательством Ставропольского края, Уставом и нормативными актами Оператора;
- обеспечение условий выполнения трудовых обязанностей сотрудников Оператора;
- организация и проведение комплекса мероприятий по формированию государственных информационных ресурсов Ставропольского края, обеспечению доступа граждан, организаций и общественных объединений к информации о деятельности государственных органов Ставропольского края, а также организации технологического обеспечения взаимодействия при предоставлении государственных услуг (функций) органами исполнительной власти Ставропольского края и подведомственными им учреждениями в электронной форме;
- организация выдачи квалифицированных электронных подписей в соответствии с Федеральным законом «Об электронной подписи» от 06 апреля 2011 года № 63-ФЗ;
- организация выдачи справочно-ключевой информации защищенных сетей ViPNet, обеспечивающих криптографическую защиту информации, передающуюся по каналам информационно-телекоммуникационной сети органов государственной власти Ставропольского края и/или подведомственных органам государственной власти Ставропольского края, государственных и муниципальных учреждений и иных организаций, участвующих в формировании инфраструктуры электронного Правительства Ставропольского края.

3. Категории ПДн

3.1. Для выполнения целей, согласно трудовому законодательству, законодательству Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, Оператором обрабатываются ПДн различных категорий субъектов:

- сотрудники Оператора: ФИО, дата рождения, место рождения, гражданство, знание иностранного языка, сведения об образовании и профессии, сведения о стаже работы, состояние в браке, состав семьи, паспортные данные, адрес места жительства и дата регистрации, телефон, сведения о воинском учёте (для мужчин), сведения об аттестации сотрудника, сведения о повышении квалификации и профессиональной переподготовке, сведения о государственных и ведомственных наградах, почетных званиях, информация об отпусках, информация о социальных льготах, сведения об увольнении (если имеются).
- ближайшие родственники сотрудников: степень родства, ФИО, год рождения.

3.1.1. В случае расторжения трудовых отношений, Оператор обрабатывает указанные ПДн в течение отчётного периода, следующего за периодом, в котором произошло расторжение трудовых отношений, для сдачи необходимой отчётности в надзорные органы. Затем указанные ПДн сдаются в архив.

3.1.2. Уничтожение ПДн в ИСПДн происходит штатными средствами ИСПДн, либо осуществляется обезличивание.

3.2. Для содействия субъекту в трудоустройстве, Оператор обрабатывает ПДн кандидатов для приёма на работу, а именно: ФИО, сведения об образовании, сведения о стаже работы, номер телефона, сведения об умениях и навыках сотрудника, иная информация, которую субъект посчитал нужным сообщить сотрудникам Оператора в целях трудоустройства.

3.2.1. Оператор обрабатывает указанные сведения в период проведения конкурса на замещение вакантных мест.

3.2.2. По достижении целей обработки, ПДн удаляются из ИСПДн штатным способом, а бумажные носители ПДн уничтожаются путём измельчения в устройстве для измельчения бумаги.

3.2.3. Если ПДн кандидата получены из общедоступных источников, то сроки их хранения не ограничиваются.

3.2.4. Формы фиксации ПДн сотрудника включают в себя: письменное заявление о приёме на работу, характеристика-рекомендация, результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей, копия приказа о приёме на работу, трудовой договор, расписка сотрудника об ознакомлении с документами Оператора, устанавливающими порядок обработки ПДн, а также о правах и обязанностях в этой области, расписка сотрудника об ознакомлении его с локальными нормативными актами Оператора, типовые формы письменного добровольного согласия на обработку получение его персональных данных согласно Приложению к настоящему Положению, корпоративный телефонный справочник.

3.3. Для выполнения целей в рамках обслуживания государственных информационных систем Ставропольского края Оператор обрабатывает ПДн субъектов, обратившихся в органы государственной власти Ставропольского края, а именно: ФИО, паспортные данные, адрес места жительства и дата регистрации, ИНН, СНИЛС

3.3.1. Оператор обрабатывает (хранит) указанные сведения по поручениям других операторов.

3.3.2. По достижении целей обработки, ПДн удаляются из ИСПДн штатным способом сотрудниками органов государственной власти Ставропольского края, либо обезличиваются.

3.4. Для выполнения целей в рамках выдачи квалифицированных электронных подписей Оператор обрабатывает ПДн субъектов, а именно: ФИО, должность, паспортные данные, ИНН, СНИЛС.

3.4.1. По достижении целей обработки, ПДн удаляются из ИСПДн штатным способом, а бумажные носители ПДн уничтожаются путём измельчения в устройстве для измельчения бумаги.

3.5. Для выполнения целей в рамках выдачи справочно-ключевой информации защищенных сетей ViPNet, обеспечивающих криптографическую защиту информации, передающуюся по каналам информационно-телекоммуникационной сети органов государственной власти Ставропольского края и/или подведомственных органам государственной власти Ставропольского края, государственных и муниципальных учреждений и иных организаций, участвующих в формировании инфраструктуры электронного Правительства Ставропольского края.

3.5.1. По достижении целей обработки, ПДн удаляются из ИСПДн штатным способом, а бумажные носители ПДн уничтожаются путём измельчения в устройстве для измельчения бумаги.

3.6. Перечень категорий ПДн может пересматриваться по мере необходимости.

4. Порядок обработки и защиты ПДн

4.1. Все ПДн Оператор получает от самих субъектов ПДн, либо от их представителей. ПДн ближайших родственников сотрудников Оператора, необходимые для ведения кадрового учёта, Оператор получает от самих сотрудников.

4.2. Сотрудники Оператора, которые работают с ПДн, получают допуск к таким данным исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей на основании перечня лиц, допущенных в работе с ПДн, который утверждается приказом руководителя Оператора.

4.3. Перечень лиц Оператора, имеющих доступ к ПДн должен поддерживаться в

актуальном состоянии.

4.4. Доступ сотрудников Оператора к ПДн прекращается с даты прекращения трудовых отношений, либо с даты изменения должностных обязанностей сотрудника и/ или исключения сотрудника из перечня лиц, имеющих право доступа к ПДн. В случае увольнения все носители, содержащие ПДн, которые в соответствии с должностными обязанностями находились в распоряжении работника во время работы, должны быть переданы соответствующему должностному лицу.

4.5. Временный или разовый допуск к работе с ПДн в связи со служебной необходимостью может быть получен сотрудником по письменному распоряжению руководителя Оператора.

4.6. Обработка ПДн осуществляется в соответствии с действующим законодательством РФ на основании согласия субъекта ПДн согласно Приложению к настоящему Положению. Форма согласия может быть отличной от указанной в настоящем Положении, при условии соблюдения требования статьи 9 закона 152-ФЗ «О персональных данных». Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих ПДн. (Например: анкеты, бланки).

4.7. Субъект ПДн принимает решение о предоставлении своих ПДн, и даёт согласие на их обработку своей волей и в своём интересе. При установлении договорных отношений с субъектом ПДн получение письменного согласия на обработку его ПДн не требуется.

4.8. В случае возникновения необходимости субъект ПДн имеет право отозвать согласие на обработку его ПДн согласно Приложению к настоящему Положению.

4.9. Оператор оставляет за собой право не осуществлять свои функции в отношении субъекта ПДн в случае предоставления неполных или недостоверных ПДн, а также в случае отказа дать письменное согласие на обработку ПДн.

4.9. Оператор дает письменное разъяснение субъекту ПДн о юридических последствиях отказа предоставить свои ПДн согласно Приложению к настоящему Положению.

4.10. ПДн субъектов обрабатываются в структурных подразделениях Оператора в соответствии с исполняемыми функциями.

4.11. При получении ПДн сотрудником Оператора проводится проверка достоверности ПДн.

4.12. Сотрудники, осуществляющие ввод ПДн в ИСПДн, несут ответственность за полноту введенной информации.

4.13. Субъекты ПДн или их законные представители несут ответственность за достоверность передаваемой сотруднику Оператора информации.

4.14. Доступ к ПДн, обрабатываемым без использования средств автоматизации, осуществляется сотрудниками, перечень которых утверждён приказом руководителя Оператора.

4.15. Доступ к ПДн, обрабатываемым в ИСПДн, осуществляется сотрудниками, перечень которых утверждён приказом руководителя Оператора.

4.16. Уполномоченные лица, допущенные к ПДн, имеют право получать только те ПДн, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц.

4.17. Обработка ПДн, осуществляемая с использованием средств автоматизации, должна выполняться в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.18. При работе в ИСПДн сотруднику запрещено демонстрировать экранные формы, содержащие ПДн лицам, не имеющим соответствующего допуска.

4.19. Обработка ПДн, 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 РФ от 15.09.2008 № 687.

4.20. Типовые формы документов с ПДн должны предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку его ПДн, – при необходимости получения письменного согласия на обработку ПДн.

4.21. ПДн при их обработке без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях ПДн.

4.22. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки.

4.23. Хранение материальных носителей ПДн осуществляется в специально оборудованных шкафах и сейфах (у ответственных сотрудников, назначенных приказом руководителя). Места хранения определяются в соответствии со списком, утвержденным приказом руководителя Оператора.

4.24. Носители ПДн не должны оставаться без присмотра. При покидании рабочего места сотрудники, осуществляющие обработку ПДн, должны убирать носители в шкаф или сейф, или иным образом ограничить несанкционированный доступ к таким носителям.

4.25. Сотрудники обязаны незамедлительно сообщить Ответственному за организацию обработки и защиты ПДн об утрате или недостаче носителей ПДн, а так же о причинах и условиях возможности утечки ПДн. В случае попытки посторонних лиц получить от сотрудника Оператора ПДн, незамедлительно известить об этом факте Ответственного за организацию обработки и защиты ПДн.

4.26. ПДн подлежат уничтожению либо обезличиванию в случаях:

- отзыва согласия субъекта ПДн;
- представления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- выявления неправомерной обработки ПДн;
- достижения целей обработки или в случае утраты необходимости в их достижении.

4.27. В срок, не превышающий 7-ми рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными неактуальными Оператор вносит в них необходимые изменения, и уведомляет субъекта ПДн о внесенных изменениях.

4.28. В случае выявление факта незаконного получения ПДн, либо неправомерной их обработки, в срок, не превышающий 10-ти рабочих дней, Оператор уничтожает такие ПДн и уведомляет субъекта ПДн об их уничтожении.

4.29. Уничтожение ПДн осуществляется в срок, не превышающий 30-ти рабочих дней с момента достижения цели обработки ПДн, с момента отзыва согласия субъекта ПДн, если иное не предусмотрено федеральными законами. По результатам уничтожения ПДн составляется акт, согласно Приложению к настоящему Положению.

4.30. Уничтожение ПДн осуществляет комиссия в составе сотрудников структурного подразделения, обрабатывавшего ПДн субъекта и установившего необходимость уничтожения ПДн под контролем руководителя этого структурного подразделения.

4.31. ПДн на бумажных носителях уничтожаются путем использования шредера (уничтожителя документов), установленного в структурном подразделении.

4.32. ПДн, размещенные на флеш-картах, CD-дисках или ином физическом носителе уничтожаются путем удаления файлов с носителя (форматировании носителя), а при необходимости, путем полного нарушения работоспособности носителя.

4.33. ПДн, размещенные в ИСПДн уничтожаются путем удаления таких данных из базы данных ИСПДн.

4.34. Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

4.35. При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путем перезаписи полей баз данных, которые позволяют определить субъекта данными, исключающими дальнейшее определение субъекта ПДн.

4.36. Контроль выполнения процедур уничтожения ПДн осуществляет руководитель структурного подразделения, сотрудник которого осуществляет обработку ПДн и определяет необходимость их уничтожения.

4.37. Все лица, допущенные к работе с ПДн, а так же связанные с эксплуатацией и техническим сопровождением ИСПДн должны быть под роспись ознакомлены с требованиями настоящего Положения, другими документами Оператора, устанавливающими порядок обработки и защиты ПДн субъектов, права и обязанности в этой области, а так же должны подписать «Обязательство о неразглашении персональных данных субъектов ГКУ СК «Краевой центр информтехнологий» согласно Приложению к настоящему Положению.

4.38. Защиту ПДн от неправомерного их использования или утраты Оператор обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

4.39. Обеспечение конфиденциальности ПДн, обрабатываемых Оператором, является обязательным требованием для всех лиц, которым ПДн стали известны.

4.40. Технические меры защиты ПДн при их обработке техническими средствами устанавливаются в соответствии с:

- постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
- внутренними документами Оператора, действующими в сфере ПДн.

4.41. При обработке ПДн в ИСПДн должно быть обеспечено:

- проведение мероприятий, направленных на предотвращения несанкционированного доступа к ПДн и/или передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к ПДн;
- недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль над обеспечением уровня защищенности ПДн.

4.42. Оператор обязан принимать необходимые правовые, организационные, технические и другие меры для обеспечения безопасности ПДн.

4.43. Защита ПДн предусматривает ограничение к ним доступа.

4.44. Порядок доступа к ПДн устанавливается пункте 5.1 – 5.7 настоящего Положения.

4.45. Ответственные за организацию обработки и защиты ПДн, администрирование средств и механизмов защиты, техническое обслуживание ИСПДн назначаются приказом руководителя Оператора.

4.46. В обязанности администраторов ИСПДн входит управление учетными записями пользователей ИСПДн, поддержание штатной работы ИСПДн, обеспечение резервного копирования данных, а так же установка и конфигурирование аппаратного и программного обеспечения ИСПДн, не связанного с обеспечением безопасности ПДн и ИСПДн.

4.47. В обязанности администратора ИСПДн входит обеспечение соответствия порядка обработки и обеспечения безопасности ПДн и ИСПДн требованиям по конфиденциальности, целостности и доступности ПДн, предъявляемым к конкретной ИСПДн, и общим требованиям по безопасности ПДн, установленным федеральным законодательством.

4.48. В обязанности администраторов ИСПДн входит учет и хранение носителей ПДн, периодический аудит журналов безопасности и анализ защищенности ИСПДн, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ПДн.

4.49. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения, критичных для безопасности ПДн, полномочий у одного лица не рекомендуется совмещать роли пользователя ИСПДн и администратора ИСПДн в лице одного сотрудника.

4.50. Руководитель структурного подразделения Оператора, осуществляющего обработку ПДн:

- несёт ответственность за организацию защиты ПДн в структурном подразделении;
- закрепляет за сотрудниками, уполномоченными обрабатывать ПДн, конкретные носители с ПДн, которые необходимы для выполнения возложенных на них функций;
- организовывает изучение уполномоченными сотрудниками нормативных правовых актов по защите ПДн и требует их неукоснительного исполнения;
- обеспечивает режим конфиденциальности в отношении ПДн, обрабатываемых в структурном подразделении;
- организовывает контроль доступа к ПДн в соответствии с функциональными обязанностями сотрудников подразделения.

4.51. Для разработки требований по обеспечению безопасности и внедрения системы обеспечения безопасности ПДн Оператором должна быть разработана «Модель угроз безопасности ПДн при их обработке в ИСПДн» для каждой ИСПДн в отдельности на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

4.52. Оператором в соответствии с руководящим документом государственных органов – Постановлением Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» должна быть осуществлена классификация каждой ИСПДн Оператора.

4.53. Комиссией должен быть составлен Акт классификации каждой ИСПДн, обрабатываемой ПДн с использованием средства автоматизации.

4.54. Оператором в конце календарного года ежегодно формируется и утверждается план мероприятий по защите ПДн и план внутренних проверок состояния защиты ПДн на следующий календарный год.

4.55. Организация внутреннего контроля процесса обработки ПДн у Оператора

осуществляется в целях изучения и оценки процесса фактического состояния защищенности ПДн, своевременного реагирования на нарушения установленного порядка их обработки, а так же в целях совершенствования этого порядка и обеспечения его соблюдения.

4.56. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ПДн направлены на решение следующих задач:

- обеспечение соблюдения сотрудниками Оператора требований настоящего Положения и нормативно-правовых актов, регулирующих сферу ПДн;
- оценка компетентности персонала, задействованного в работе с ПДн;
- обеспечение работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ПДн;
- выявление нарушений установленного порядка обработки ПДн и своевременного предотвращение негативных последствий таких нарушений;
- принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки ПДн, так и в работе технических средств ИСПДн;
- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ПДн по результатам контрольных мероприятий;
- осуществление внутреннего контроля за исполнением рекомендаций и указаний по устранению нарушений.

4.57. Оператором используются технические средства защиты информации (в том числе криптографические) для обработки и обеспечения безопасности ПДн. Ведутся соответствующие журналы учета средств защиты (в том числе криптографических).

4.58. Вышеуказанные технические средства защиты информации (в том числе криптографические) размещаются исключительно в пределах утвержденных границ контролируемой зоны Оператора.

4.59. Уполномоченным сотрудником Оператора должен вестись журнал учета и хранения съёмных носителей конфиденциальной информации (в том числе ПДн).

4.60. Помещения Оператора, в конце рабочего дня и при отсутствии сотрудников в помещениях, должны запираться, окна должны быть закрыты, должна быть включена сигнализация.

4.61. Доступ в специальные помещения (в том числе помещения серверной) должен быть ограничен.

4.62. Уборка помещений и обслуживание технических средств ИСПДн должна осуществляться под контролем ответственных за данное помещение лиц с соблюдением мер, исключающих несанкционированный доступ к ПДн, носителям ПДн, программным и техническим средствам обработки, передачи и защиты ПДн.

4.63. Список сотрудников Оператора, имеющих право доступа в помещения, где ведется работа с ПДн, должен быть утвержден приказом руководителя Оператора.

5. Особенности управления ПДн сотрудников Оператора

5.1. ПДн сотрудников Оператора – информация необходимая Оператору в связи с трудовыми отношениями и касающаяся конкретного сотрудника.

5.2. Обработка ПДн сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудников в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля качества и количества выполняемой работы и обеспечения сохранности имущества.

5.3. Оператор не имеет право получать и обрабатывать ПДн сотрудника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

5.4. При принятии решений, затрагивающих интересы сотрудника, Оператор не имеет права основываться на ПДн сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.5. Сотрудники не должны отказываться от своих прав на сохранение и защиту сведений о фактах, событиях и обстоятельствах его частной жизни, личной и/или семейной тайны.

5.6. Оператор обязуется не сообщать ПДн сотрудника иным организациям без его письменного согласия.

5.7. Оператор обязуется предупредить своих сотрудников, третьих лиц, получающих ПДн сотрудника (при его письменном согласии), о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн сотрудника, обязаны соблюдать режим конфиденциальности таких данных, который обеспечивается подписанием с лицом Обязательства о неразглашении согласно Приложению к настоящему Положению, за исключением случаев обмена ПДн сотрудников в порядке, установленном законодательством РФ.

5.8. Оператор обязуется не запрашивать информацию о состоянии здоровья сотрудника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции.

5.9. Сотрудник имеет право на определение своих представителей для защиты своих ПДн.

6. Правила работы с обезличенными данными

6.1. Порядок обезличивания ПДн включает в себя замену идентифицирующей информации о субъекте ПДн (например: Фамилию, Имя и Отчество) на произвольный код (далее – идентификатор).

6.2. Обезличивание должно проводиться таким образом, чтобы определить принадлежность ПДн конкретному субъекту ПДн было невозможно без использования дополнительной информации.

6.3. Способы обезличивания при условии дальнейшей обработки ПДн:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- деление сведений на части и обработка в разных ИСПДн;
- другие способы.

6.4. Если обезличенные ПДн используются в статистических или иных исследовательских целях, сроки обработки и хранения ПДн устанавливаются руководством Оператора исходя из служебной необходимости, и получение согласия субъекта на обработку его ПДн не требуется на основании Федерального Закона №152-ФЗ от 26.07.2006 «О персональных данных».

6.5. Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных ПДн в ИСПДн и целесообразность их применения определяются Ответственным за организацию обработки и защиты ПДн индивидуально для каждой ИСПДн.

6.6. При обработке обезличенных ПДн с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;

- правил доступа в помещения, где расположены элементы ИСПДн.

6.7. При обработке обезличенных ПДн правил хранения бумажных носителей;

- правил доступа к ним и в помещения, где они хранятся.

6.8. Обезличенные ПДн не подлежат разглашению и нарушению их конфиденциальности.

6.9. В случае достижения целей обработки ПДн или в случае утраты необходимости в их достижении ответственный сотрудник, назначенный приказом руководителя Оператора, обязан:

- незамедлительно прекратить обработку ПДн;
- обезличить либо уничтожить соответствующие ПДн в срок, не превышающий 30 дней с даты достижения целей обработки ПДн.

6.10. ПДн не обезличиваются (не уничтожаются) в случаях, если:

- договором, соглашением стороной которого, выгодоприобретателем или поручителем является субъект персональных данных, предусмотрен иной порядок обработки ПДн;
- законодательством установлены сроки обязательного архивного хранения материальных носителей ПДн;
- в иных случаях, прямо предусмотренных законодательством.

6.11. Перечень лиц, имеющих право обезличивать ПДн, утверждается руководителем Оператора.

7. Передача ПДн третьим лицам

7.1. Доступ к ПДн третьих лиц, не являющихся сотрудниками Оператора без письменного согласия субъекта ПДн согласно Приложению к настоящему Положению, запрещен, за исключением доступа сотрудников органов исполнительной власти, осуществляемого в рамках мероприятий по контролю и надзору за исполнением законодательства, реализации функций и полномочий соответствующих органов государственной власти. Предоставление информации по запросу или требованию органа государственной власти осуществляется по согласованию руководителя Оператора. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Оператором и субъектом ПДн.

7.2. На основании дополнительного соглашения согласно Приложению к настоящему Положению Оператор может поручать обработку ПДн третьим лицам. Лицо, осуществляющее обработку ПДн по поручению Оператора, обязано соблюдать порядок обработки и защиты ПДн, предусмотренный настоящим Положением.

7.3. Получение ПДн у третьих лиц, возможно только при уведомлении субъекта ПДн согласно Приложению к настоящему Положению об этом заранее и с его письменного согласия. Форма согласия может быть отличной от указанной в настоящем Положении, при условии соблюдения требования статьи 9 закона «О персональных данных». Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих ПДн субъекта (Например: анкеты, бланки).

7.4. В случае если сторонней организации необходим доступ к ПДн Оператора, в договоре с такой организацией обязательны условия конфиденциальности передаваемых ПДн, перечень требований по соблюдению текущего законодательства в сфере ПДн.

8. Права субъектов ПДн

8.1. В целях обеспечения своих интересов субъекты ПДн имеют право:

- на получение информации от Оператора, касающейся обработки его ПДн. Сведения должны быть предоставлены субъекту ПДн Оператором в доступной форме, в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением

случаев, если имеются законные основания для рассылки таких ПДн. Перечень сведений и порядок получения предусмотрен действующим законодательством РФ;

- требовать от Оператора уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством РФ меры по защите своих прав;
- на условие письменного согласия при принятии на основании исключительно автоматизированной обработки ПДн решений Оператора, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающие его права и законные интересы;
- заявлять возражения на решения Оператора на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения;
- обжаловать действия или бездействия Оператора в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

9. Права и обязанности Оператора

9.1. Оператор вправе:

- поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта;
- в случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, указанных в законодательстве РФ;
- отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством РФ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Операторе;
- самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора в области обеспечения безопасности ПДн, предусмотренных законодательство РФ;

9.2. Оператор обязан:

- до начала обработки ПДн уведомить уполномоченный органа по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством РФ;
- при получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством РФ;
- представлять доказательства получения согласия субъекта ПДн на обработку его ПДн или доказательства наличия законных оснований обработки ПДн без согласия субъекта ПДн;
- разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражения против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов;
- рассмотреть возражение субъекта ПДн в течение 30-ти рабочих дней со дня его получения и уведомить субъекта ПДн о результатах рассмотрения такого возражения;
- при сборе ПДн предоставить субъекту ПДн по его письменной просьбе информацию, предусмотренную законодательством РФ;
- если ПДн получены Оператором не от субъекта ПДн, за исключением случаев, предусмотренных законодательством РФ, до начала обработки таких ПДн, предоставить

субъекту ПДн следующую информацию:

- наименование Оператора, его юридический и фактический адрес
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленныйе федеральным законом права субъекта ПДн;
- источники получения ПДн.

- принимать меры необходимые и достаточные для обеспечения выполнения обязанностей Оператора, предусмотренные законодательством РФ;
- опубликовать на официальном сайте Оператора, обеспечив неограниченный доступ, документ, определяющий его политику в отношении обработки и защиты ПДн Оператора в течение 10 рабочих дней с момента утверждения такого документа;
- представить документы или локальные акты, предусмотренные законодательством РФ и/или иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей Оператора в области защиты ПДн по запросу уполномоченного органа по защите прав субъектов ПДн в течение 30-ти дней с даты получения запроса;
- принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничижения, блокирования, копирования, представления, распространения, а так же от иных неправомерных действий в отношении ПДн;
- сообщить в порядке, предусмотренном законодательством РФ, субъекту ПДн или его законному представителю информацию (на безвозмездной основе) о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя, либо в течение 30-ти дней с даты получения запроса субъекта ПДн или его представителя;
- в случае отказа в предоставлении информации о наличии ПДн о соответствующем субъекте ПДн или ПДн субъекту ПДн или его законному представителю при их обращении, либо получении запроса от них, дать в письменной форме мотивированный ответ, содержащий ссылку на положение законодательства РФ, являющегося основанием для такого отказа, в срок не превышающий 30-ти рабочих дней со дня обращения субъекта ПДн или его законного представителя, либо с даты получения запроса;
- в срок, не превышающий 7-ми рабочих дней со дня предоставления субъектом ПДн или его законным представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, внести с них необходимые изменения.
- в срок, не превышающий 7-ми рабочих дней со дня представления субъектом Пдн или его законным представителем сведений подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие ПДн, уведомить субъекта ПД и его законного представителя о внесённых изменениях и предпринятых мерах;
- в срок, не превышающий 3-х рабочих дней с даты выявления неправомерной обработки ПДн, обязан прекратить такую обработку или обеспечить ее прекращение если иное не предусмотрено законодательством РФ. В случае, если обеспечить правомерность обработки ПДн невозможно, в срок, не превышающий 10-ти рабочих дней с даты выявления неправомерной обработки ПДн, обязать уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн обязать уведомить субъекта ПДн или его законного представителя, а в случае, если запрос был направлен уполномоченным органом по защите прав субъектов ПДн, так узнанный орган;
- в срок, не превышающий 30-ти рабочих дней с даты достижения целей обработки ПДн, обязан прекратить такую обработку ПДн или обеспечить ее прекращение, если иное не предусмотрено законодательством РФ;
- в срок, не превышающий 30-ти рабочих дней с даты поступления отзыва субъекта

ПДн согласия на обработку его ПДн, прекратить их обработку или обеспечить ее прекращение, а в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить такие ПДн или обеспечить их уничтожение, если иное не предусмотрено законодательством РФ;

- назначить лицо, Ответственное за организацию обработки и защиты ПДн.

10. Правила рассмотрения запросов субъектов ПДн или их законных представителей

10.1. При обращении либо письменном запросе субъекта ПДн или его законного представителя, на доступ к своим ПДн Оператор руководствуется требованиями Федерального закона № 152-ФЗ от 26.07.2006 «О персональных данных».

10.2. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн Оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые Оператором способы обработки ПДн;
- наименование и место нахождения Оператора, сведения о лицах (за исключением сотрудников Оператора), которые имеют доступ к ПДн субъекта или которым могут быть раскрыты ПДн на основании договора с Оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки хранения;
- порядок осуществления субъектом ПДн прав, предусмотренных действующим законодательством;
- информацию об осуществленной или о предполагаемой трансграничной передаче ПДн;
- наименование или ФИО и адрес лица, осуществляющего обработку ПДн по поручению Оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные действующим законодательством РФ.

10.3. Доступ субъекта ПДн или его законного представителя к своим ПДн Оператор предоставляет только под контролем Ответственного за организацию обработки и защиты ПДн Оператора.

10.4. Обращение субъекта ПДн или его законного представителя фиксируются в журнале учета обращений граждан (субъектов ПДн) по вопросам обработки ПДн.

10.5. Письменный запрос субъекта ПДн или его законного представителя журнале регистрации письменных запросов граждан на доступ к своим ПДн.

10.6. ПДн могут быть предоставлены субъекту таких данных или его представителю Оператором при обращении либо при получении запроса, который должен содержать следующую информацию:

- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения);
- иные сведения, подтверждающие факт обработки ПДн Оператором;
- подпись субъекта ПДн или его представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

10.7. Ответственный за организацию обработки и защиты ПДн принимает решение о

предоставлении доступа субъекта к ПДн.

10.8. Субъект ПДн вправе обратиться повторно к Оператору или направить ему повторный запрос в целях получения сведений о его ПДн и ознакомления с такими ПДн не ранее чем через 30 дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, поручителем по которому является субъект ПДн или сведения о его ПДн не были предоставлены для ознакомления в полном объеме по результатам рассмотрения первоначального обращения.

10.9. Оператор вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, описанным раннее. В случае отказа Оператор обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение Федеральных законов, в срок, не превышающий 30-ти дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

10.10. Оператор освобождается от обязанности предоставить субъекту ПДн следующие сведения:

- наименование либо ФИО и адрес Оператора или его представителя;
- цель обработки ПДн и ее правовое основание;
- предполагаемые пользователи ПДн;
- установленные Федеральным законом права субъекта ПДн;
- источник получения ПДн;

в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его ПДн соответствующим Оператором;
- ПДн получены Оператором на основании федерального закона или в связи с исполнением договора, поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника.
- Оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

10.11. Оператор в срок, не превышающий 7-ми рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, вносит в них необходимые изменения и уничтожает ПДн, в случае предоставления сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

10.12. В случае, если данных предоставленных субъектом не достаточно для установления его личности или предоставление ПДн нарушает конституционные права и свободы других лиц Ответственный за организацию обработки и защиты ПДн подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 федерального закона «О персональных данных» или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 рабочих дней со дня обращения субъекта ПДн или его законного представителя либо от даты получения запроса субъекта ПДн или его законного представителя.

10.13. Для предоставления доступа субъекта ПДн или его законного представителя к ПДн субъекта Ответственный за организацию обработки и защиты ПДн привлекает сотрудника (сотрудников) структурного подразделения, обрабатывающего ПДн субъекта по согласованию с руководителем этого структурного подразделения.

10.14. Сведения о наличии ПДн Оператора предоставляет субъекту ПДн в доступной

форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн. Контроль предоставления сведений субъекту или его законному представителю осуществляет Ответственный за организацию обработки и защиты ПДн.

11. Порядок действий в случае запросов надзорных органов

11.1. В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ «О персональных данных» Оператор обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30-ти дней с даты получения такого запроса.

11.2. Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет Ответственный за организацию обработки и защиты ПДн при необходимости с привлечением сотрудников Оператора.

11.3. В течение установленного законодательством срока Ответственный за организацию обработки и защиты ПДн подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

12. Порядок доступа лиц в помещения, в которых ведётся обработка персональных данных

12.1. Помещения, в которых ведется обработка ПДн, являются помещениями с ограниченным доступом (далее – специальные помещения). Бесконтрольный доступ посторонних лиц в специальные помещения должен быть исключён.

12.2. Доступ в специальные помещения, разрешён только перечню лиц, который утвержден в соответствии с приказом руководителя Оператора (далее – Перечень).

12.3. Уборка специальных помещений происходит только при строгом контроле указанных в Перечне лиц.

12.4. Специальными помещениями являются:

- помещения, в которых происходит обработка ПДн, как с использованием средств автоматизации, так и без таковых;
- помещения, аттестованные по требованиям безопасности информации (далее – защищаемые помещения);
- помещения, в которых установлены компьютеры, сервера и коммутационное оборудование, участвующее в обработке ПДн;
- помещения, в которых хранятся материальные носители ПДн;
- помещения, в которых хранятся резервные копии ПДн.

12.5. Специальные помещения должны быть оборудованы охранной сигнализацией, двери в такие помещения должны иметь средство для опечатывания или аппаратное техническое средство, предназначенное для ограничения доступа посторонних лиц в такие помещения.

12.6. Сотрудники структурных подразделений Оператора, на которых возложена обязанность по обработке ПДн, несут персональную ответственность за выполнение мероприятий по предотвращению несанкционированного доступа к обрабатываемым ПДн лицами, которые не допущены к их обработке и /или ознакомлению.

12.7. Доступ сотрудников Оператора в специальные помещения осуществляется для выполнения ими своих служебных обязанностей и возложенных на них функций, согласно Перечню.

12.8. Допуск сотрудников в специальные помещения оформляется после подписания таким сотрудником обязательства о неразглашении и инструктажа Ответственного за организацию обработки и защиты ПДн, либо администратора информационной безопасности Оператора.

12.9. Доступ посторонних лиц в специальные помещения должен осуществляться только ввиду служебной необходимости и в присутствии допущенных сотрудников Оператора.

12.10. Ознакомление с ПДн лиц прибывших для проведения контрольных мероприятий, осуществляется в объеме, предусмотренном планом проверки.

12.11. На момент присутствия посторонних лиц в специальных помещениях должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн.

12.12. В нерабочее время специальные помещения должны быть опечатаны и поставлены на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители ПДн (в том числе документы с ПДн) должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены.

12.13. Сдачу (вскрытие) специальных помещений под охрану осуществляют сотрудники структурных подразделений Оператора, согласно Перечню с отметкой в журнале вскрытия/ опечатывания помещений на посту охраны.

12.14. При вскрытии специальных помещений, сотрудники обязаны сделать запись в журнале вскрытия/опечатывания помещений на посту охраны, проверить целостность печати перед вскрытием, визуально проверить помещение на предмет несанкционированного проникновения.

12.15. При обнаружении признаков, указывающих на возможное несанкционированное проникновение посторонних лиц в специальные помещения, о случившемся должно быть немедленно сообщено Ответственному за организацию обработки и защиты ПДн. Прибывший Ответственный за организацию обработки и защиты ПДн должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации ПДн.

12.16. Размещение и монтаж технических средств с целью обеспечения безопасности ПДн должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования осуществляются лицами, имеющими право на обслуживание таких средств.

12.17. На время отсутствия пользователей ПДн указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Ответственным за организацию обработки и защиты ПДн необходимо предусмотреть организационно-технические меры, исключающие возможность использования технического оборудования посторонними лицами.

13. Резервное копирование и восстановление персональных данных, обрабатываемых в информационных системах персональных данных

13.1. Резервному копированию подлежат все информационные ресурсы Оператора, содержащие ПДн субъектов, а именно:

- файлы баз данных;
- электронные документы;
- отсканированные и хранящиеся в ИСПДн изображения документов и фотографии субъектов.

13.2. Резервному копированию могут так же подвергаться:

- системное и прикладное программное обеспечение ИСПДн;
- средства защиты информации в ИСПДн.

13.3. Резервирование информационных ресурсов ИСПДн, содержащих ПДн (далее – резервирование ПДн), выполняется Администратором ИСПДн.

13.4. Определяется 2 вида резервирования ПДн:

- полное резервирование – резервное копирование всех ПДн, хранящихся в ИСПДн;
- неполное резервирование – резервное копирование части ПДн, хранящихся в ИСПДн.

13.5. Целью неполного резервирования является сохранение изменений в ИСПДн с момента полного резервирования ПДн.

13.6. Периодичность проведения работ по резервированию ПДн определяется Администратором ИСПДн с учётом специфики работы ИСПДн, но не менее 1 раза в месяц для полного резервирования и 1 раза в неделю для неполного резервирования.

13.7. В случаях, когда ПДн хранятся на компьютерах пользователей ИСПДн локально, допустимо перекладывать ответственность за проведение неполного резервирования ПДн на пользователей ИСПДн.

13.8. События резервирования ПДн фиксируются в Журнале резервирования информационных ресурсов ИСПДн, содержащих ПДн. В журнале указывается: дата, вид резервирования, наименование резервируемого информационного ресурса, количество и общий размер файлов, серийный номер носителя информации, ответственное лицо.

13.9. Администратор ИСПДн может использовать средства резервного копирования ИСПДн для резервирования ПДн на отчуждаемый носитель. В случаях, когда резервирование ПДн средствами ИСПДн не представляется возможным, администратор ИСПДн по согласованию с Ответственным за организацию обработки и защиты ПДн может использовать средство резервного копирования, не входящее в состав ИСПДн.

13.10. Резервное копирование с использованием незащищённых каналов связи общего пользования не допустимо.

13.11. Резервное копирование по локальной сети на устройство, находящееся вне ИСПДн, не допустимо.

13.12. При резервировании ПДн не допускается хранение на одном носителе резервных копий ПДн, извлечённых из различных ИСПДн. Для осуществления резервирования ПДн различных ИСПДн, для каждой ИСПДн должен быть предусмотрен отдельный носитель информации.

13.13. В случае удаления ПДн субъекта из ИСПДн должна быть так же удалена резервная копия этих данных.

13.14. Хранение резервных копий ПДн должно исключать любой несанкционированный доступ посторонних лиц к носителям информации.

13.15. Хранение резервных копий необходимо осуществлять в сейфах, несгораемых шкафах, металлических шкафах с устройством опечатывания. Доступ к местам хранения резервных копий должен быть предоставлен только Администратору ИСПДн.

13.16. Не допускается хранение резервных копий ПДн совместно с другими носителями информации.

13.17. На носителе информации, содержащем резервные копии ПДн, не должна храниться посторонняя информация.

13.18. Должно быть обеспечено одновременное хранение не менее двух носителей информации, хранящих полную резервную копию ПДн ИСПДн.

13.19. В случае сбоя в работе ИСПДн, восстановление ПДн из резервных копий осуществляет Администратор ИСПДн.

13.20. Администратор ИСПДн обязан срочно уведомить Ответственного за организацию обработки и защиты ПДн о факте сбоя в работе ИСПДн, повлёкшего нарушение целостности ПДн.

13.21. Факты восстановления ПДн должны фиксироваться Администратором ИСПДн в Журнале резервирования информационных ресурсов ИСПДн, содержащих ПДн (в графе «вид резервирования» указывается «полное восстановление» либо «частичное восстановление»).

13.22. Временной норматив по восстановлению ПДн устанавливается Ответственным

за организацию обработки и защиты ПДн с учётом специфики работы ИСПДн.

14. Обязанности лиц, допущенных к обработке ПДн

14.1. Лица, допущенные к работе с ПДн, обязаны:

- знать законодательство Российской Федерации в области обработки и защиты ПДН, нормативные документы Оператора по защите ПДн;
- сохранять конфиденциальность ПДн;
- обеспечивать сохранность закреплённых за ними носителей ПДн;
- контролировать срок истечения действия согласий на обработку ПДн и, при необходимости дальнейшей обработки ПДн, обеспечивать своевременное получение новых согласий или прекращение обработки ПДн;
- докладывать своему непосредственному руководителю отдела (структурного подразделения) обо всех фактах и попытках несанкционированного доступа к ПДн и других нарушениях.

15. Функциональные обязанности ответственного за организацию обработки и защиты персональных данных

15.1. Ответственный за организацию обработки и защиты ПДн должен быть сотрудником Оператора, который назначается приказом руководителя Оператора.

15.2. Деятельность Ответственного за организацию обработки и защиты ПДн осуществляется согласно плану мероприятий по защите ПДн, утвержденного руководителем Оператора на календарный год.

15.3. На Ответственного за организацию обработки и защиты ПДн возложены следующие задачи:

- организация внутреннего контроля за соблюдением сотрудниками Оператора норм законодательства Российской Федерации по сфере ПДн, в том числе требований, предъявляемых к защите ПДн;
- разработка, внедрение и актуализация локальных актов в сфере ПДн;
- доведение до сведения сотрудников Оператора, непосредственно осуществляющих работу с ПДн, положений законодательства Российской Федерации о ПДн, требований Положения о порядке обработки и защите персональных данных, утвержденного руководителем Оператора и иных локальных актов Оператора в сфере ПДн, и проведение обучения указанных сотрудников;
- организация приема и обработки обращений и запросов субъектов ПДн или их представителей и осуществление контроля за приемом и обработкой таких обращений и запросов;
- организация комплексной защиты информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих ПДн субъектов Оператора;
- организация защиты средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой информации),

используемых для реализации процессов ведения деятельности, обработки информации, содержащей ПДн субъектов Оператора;

- организация защиты ПДн субъектов Оператора;
- разработка и проведение организационных мероприятий, обеспечивающих безопасность ПДн, своевременное выявление и устранение возможных каналов утечки информации;
- организация проведения работ по технической защите ПДн на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Оператора;
- реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в структурных подразделениях Оператора;
- методическое руководство системой обеспечения защиты ПДн Оператора;
- организация контроля состояния и проведения оценки эффективности системы обеспечения безопасности ПДн, а также реализация мер по её совершенствованию;
- внедрение в информационную инфраструктуру Оператора современных методов и средств обеспечения защищённости ПДн;

15.4. Для решения поставленных задач Ответственный за организацию обработки и защиты ПДн осуществляет функции:

- разработка и внедрение правовых, организационных и технических мер по комплексному обеспечению безопасности ПДн;
- обеспечение соблюдения режима конфиденциальности при обработке ПДн;
- планирование работы по защите ПДн на объектах Оператора;
- контроль за выполнением мер по защите ПДн, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;
- контроль за выполнением плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите ПДн, выполняемых контрагентами;
- проведение работ по технической защите ПДн на объектах информатизации Оператора. Оценка эффективности принятых мер по технической защите информации;
- обеспечение выбора, установки, настройки и эксплуатации средств защиты ПДн в соответствии с организационно-распорядительной и эксплуатационной документацией.
- организация режима обеспечения безопасности помещений, в которых происходит обработка ПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения.
- организация доступа сотрудников Оператора к ПДн в соответствии с возложенными на них служебными обязанностями.
- разработка и внедрение локальных актов, определяющих перечень сотрудников Оператора, имеющих доступ к ПДн.
- контроль размещения устройств ввода (отображения) информации, исключающего ее несанкционированный просмотр.
- обеспечение соответствия проводимых работ по защите ПДн технике безопасности, правилам и нормам охраны труда.
- проведение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства по защите ПДн.
- участие в разработке и применение, в части ПДн, политики по работе с инцидентами по информационной безопасности.
- актуализация внутренней организационно-распорядительной документации по защите ПДн при изменении существующих и выходе новых нормативных правовых документов по вопросам обработки ПДн.

15.5. Ответственный за организацию обработки и защиты ПДн имеет право:

- осуществлять контроль за деятельностью структурных подразделений Оператора по выполнению ими требований по защите ПДн.
- составлять акты, докладные записки, отчёты для рассмотрения руководством Оператора, при выявлении нарушений порядка обработки ПДн.
- принимать необходимые меры при обнаружении несанкционированного доступа к ПДн, как сотрудниками Оператора, так и третьими лицами, и докладывать о принятых мерах руководителю Оператора с предоставлением информации о субъектах, нарушивших режим доступа.
- вносить на рассмотрение руководителя Оператора предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа.
- давать структурным подразделениям Оператора, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного а организацию обработки и защиты ПДн.
- запрашивать и получать от всех структурных подразделений Оператора сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного а организацию обработки и защиты ПДн.
- составлять акты и другую техническую документацию о степени защищенности объектов информатизации.
- готовить и вносить предложения на проведение работ по защите ПДн, о привлечении к проведению работ по оценке эффективности защиты ПДн на объектах Оператора (на договорной основе) организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат качества.
- осуществлять визирование договоров с контрагентами с целью правового обеспечения передачи им ПДн субъектов Оператора в ходе выполнения работ по этим договорам.
- представлять интересы Оператора при осуществлении государственного контроля и надзора за обработкой ПДн Уполномоченным органом по защите прав субъектов ПДн.

15.6. Ответственный за организацию обработки и защиты ПДн выполняет свои задачи, осуществляя взаимодействие со всеми структурными подразделениями Оператора.

15.7. Для выполнения своих функций и реализации предоставленных прав Ответственный за организацию обработки и защиты ПДн взаимодействует с территориальными и региональными подразделениями ФСТЭК России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, ФСБ России, МВД России, и другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты ПДн на законном основании.

15.8. Ответственный за организацию обработки и защиты ПДн несет ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации обработки ПДн Оператора в соответствии с положениями законодательства Российской Федерации в области ПДн.

16. Ответственность сотрудника за нарушение норм, регулирующих обработку и защиту ПДн

16.1. Руководство Оператора несет ответственность за необеспечение конфиденциальности ПДн и несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

16.2. Сотрудники Оператора несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ПДн, установленных настоящим

Положением, в соответствии с законодательством РФ.

16.3. Сотрудник Оператора может быть привлечен к ответственности в следующих случаях:

- умышленного или неосторожного раскрытия ПДн;
- утраты материальных носителей ПДн;
- нарушения требований настоящего Положения и других нормативных документов Оператора в части вопросов доступа и работы с ПДн.

16.4. В случаях нарушения установленного порядка обработки и обеспечения безопасности ПДн, несанкционированного доступа к ПДн, раскрытия ПДн и нанесения Оператору, его сотрудникам, субъектам ПДн материального или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную или иную предусмотренную законодательством Российской Федерации ответственность.

17. Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн

17.1. В целях осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн Оператор организовывает проведение плановых и внеплановых проверок условий обработки ПДн на предмет соответствия Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных данных», принятым в соответствии с ним нормативным правовым актам и локальными актами Оператора (далее – Проверки).

17.2. Проверки, установленные Оператором проводятся Ответственным за организацию обработки и защиты ПДн на основании ежегодного плана (далее – плановые проверки) или на основании поступившего Оператору письменного заявления о нарушениях правил обработки ПДн (далее – внеплановые проверки).

17.3. Контроль выполнения требований по защите ПДн в структурных подразделениях Оператора имеет целью определить наличие несоответствий между требуемым уровнем защиты ПДн и его фактическим состоянием, а также выработать меры по их устранению и недопущению в дальнейшем таких несоответствий.

17.4. Проверки осуществляются Ответственным за организацию обработки и защиты ПДн непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПДн.

17.5. Порядок подготовки к проверке:

- Для участия в проведении проверки Ответственным за организацию обработки и защиты ПДн заблаговременно определяются соответствующие компетентные специалисты (далее – проверяющие лица) при необходимости. В случае проведения проверки комиссией приказом руководителя Оператора назначается председатель и её состав.
- Председатель комиссии распределяет обязанности по проверке конкретных участков работы между проверяющими лицами.
- Проверяющие лица инструктируются Ответственным за организацию обработки и защиты ПДн об особенностях работы в конкретном подразделении Оператора. За 3 – 4 дня до начала проверки проверяющие лица должны изучить материалы предыдущих проверок данного подразделения, уточнить наличие в нем защищаемых ресурсов, сил и средств защиты ПДн, а также особенности их функционирования.
- По итогам проверки Ответственным за организацию обработки и защиты ПДн (в случае назначения комиссии – председателем) составляется акт только в случае выявления нарушений. Если нарушений не выявлено, Ответственный за организацию обработки и защиты ПДн (в случае назначения комиссии – председатель) докладывает всю необходимую информацию руководителю Оператора в той форме, которую установит руководитель самостоятельно.

17.6. В ходе осуществления контроля выполнения требований по защите ПДн в подразделении Оператора проверке подлежат следующие показатели:

В части общей организации работ по защите ПДн:

- соответствие информации, указанной в уведомлении об обработке ПДн, реальному положению дел;
- знание нормативных документов сотрудниками, имеющими доступ к ПДн;
- полнота и правильность выполнения требований нормативных документов сотрудниками, имеющими доступ к ПДн;
- наличие лиц, назначенных Ответственным за организацию обработки и защиты ПДн в подразделении, уровень их профессиональной подготовки и способность выполнить возложенные обязанности;
- наличие согласий на обработку ПДн субъектов ПДн. Соответствие объёма ПДн и сроков обработки целям обработки ПДн;
- соответствие схемы контролируемой зоны, перечня мест хранения материальных носителей, перечня лиц, допущенных к обработке ПДн фактическому состоянию.

В части защиты ПДн в ИСПДн:

- соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;
- структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) ПДн в сети передачи данных;
- контроль целостности пломб на автоматизированных рабочих местах (далее – АРМ) пользователей, с которыми осуществляется штатное функционирование средств криптографической защиты информации с целью обеспечения безопасности ПДн;
- соблюдение установленного порядка использования АРМ, имеющих доступ к ИСПДн;
- наличие и эффективность применения средств и методов защиты ПДн, обрабатываемых на АРМ пользователей;
- соблюдение требований, предъявляемых к паролям в ИСПДн;
- контроль журналов учёта носителей ПДн. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

В части защиты информационных ресурсов и помещений:

- правильность отнесения обрабатываемой информации к ПДн;
- закрепление гражданско-правовой ответственности в сфере ПДн в правилах внутреннего трудового распорядка, положениях о подразделениях Оператора, должностных инструкциях сотрудников и трудовых договорах;
- порядок передачи ПДн;
- действенность принимаемых мер по защите ПДн в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;
- выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки ПДн при проведении мероприятий конфиденциального характера.

17.7. Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

17.8. В ходе работы проверяющие лица должны принимать меры по устранению на месте отмечаемых нарушений и недостатков. Для этого с должностными лицами подразделения, ответственными за конкретные участки работы, где отмечались недостатки, одновременно должны проводиться разъяснения требований руководящих документов и оказываться практическая помощь в правильной постановке работы

17.9. В случае выявления фактов:

- несоблюдения установленного порядка обработки ПДн;

- несоблюдения условий хранения носителей ПДн;
- использования средств защиты информации, приводящие к нарушению заданного уровня безопасности (конфиденциальность/целостность/доступность) ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн;
- нарушения заданного уровня безопасности ПДн;

в обязательном порядке устанавливаются причины нарушения обработки ПДн и наличие (отсутствие) вины.

17.10. В процессе проведения внутреннего контроля (проверок) соответствия обработки ПДн требованиям к защите ПДн разрабатываются меры, направленные на предотвращение негативных последствий выявленных нарушений.

17.11. В случаях выявления нарушений обработки ПДн, требующих немедленного устранения, принимаются меры оперативного реагирования.

Приложение №1
к настоящему Положению

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
проживающий (– ая) по адресу_____
_____,
паспорт серии _____, номер _____, выдан_____
_____
«___»_____ _____ года, в соответствии с в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях:

- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;
- предоставления сведений в банк для оформления банковской карты и перечисления на нее заработной платы;
- предоставления сведений третьим лицам для оформления полиса ДМС;
- предоставления налоговых вычетов;
- обеспечения моей безопасности;
- контроля количества и качества выполняемой мной работы;
- обеспечения сохранности имущества работодателя

ДАЮ СОГЛАСИЕ
ГКУ СК «Краевой центр информтехнологий», расположенному по адресу 355045, Ставропольский край, г. Ставрополь, ул. Пирогова, д. 18/6, на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Перечень моих персональных данных, на обработку которых я даю согласие: фамилия, имя, отчество; пол, возраст; дата и место рождения, паспортные данные, адрес регистрации по месту жительства и адрес фактического проживания, номер телефона (домашний, мобильный), данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации; семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления мне льгот, предусмотренных трудовым и налоговым законодательством; отношение к воинской обязанности; сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы; СНИЛС; ИНН; информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГКУ СК «Краевой центр информтехнологий»; сведения о доходах в ГКУ СК «Краевой центр информтехнологий»; сведения о деловых и иных личных качествах, носящих оценочный характер.

Настоящие согласие действует со дня его подписания до дня отзыва в письменной форме.

«___»_____ 20__г. _____

(подпись)

Приложение №2
к настоящему Положению

ОТЗЫВ СОГЛАСИЯ
на обработку персональных данных

Я, _____,
проживающий (– ая) по адресу_____
_____,
паспорт серии _____, номер _____, выдан_____
_____
«___»_____ _____ года, в соответствии с п. 1 ст. 9 Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006 года отзываю у ГКУ СК «Краевой центр информтехнологий» согласие на обработку моих персональных данных.

Прошу прекратить обработку моих персональных данных в течение трех рабочих дней с момента поступления настоящего отзыва.

«___»_____ 20__г. _____
(подпись)

Приложение №3
к настоящему Положению

СОГЛАСИЕ
на получение персональных данных от третьих лиц

Я, _____,
проживающий (– ая) по адресу_____
_____,
паспорт серии _____, номер _____, выдан_____
_____
«___»_____ _____ года, в соответствии с в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

ДАЮ СОГЛАСИЕ

ГКУ СК «Краевой центр информтехнологий», расположенному по адресу 355045, Ставропольский край, г. Ставрополь, ул. Пирогова, д. 18/6, на получение моих персональных данных о предыдущих местах работы и периодах трудовой деятельности от третьих лиц.

«___»_____ 20__г. _____
(подпись)

Приложение №4
к настоящему Положению

Уведомление о получении
персональных данных
от третьих лиц
(образец заполнения)

—

_____
_____

ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ СТАВРОПОЛЬСКОГО КРАЯ «КРАЕВОЙ ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

355045, г. Ставрополь, ул. Пирогова, 18/6
Тел.: (8652) 55-42-80, факс: (8652) 55-42-11
ОКПО 90937070, ОГРН 1112651017401
ИНН/КПП 2635805516/263501001

№ _____ от _____
На №_____от _____

О получении персональных данных
от третьих лиц

Уважаемый (-ая) _____!

Уведомляем Вас о том, что в соответствии с _____
_____
ГКУ СК «Краевой центр информтехнологий» запросит ваши персональные данные от третьих лиц. Данные сведения будут запрошены в целях _____
_____.
Сведения будут запрашиваться в письменной форме при помощи средств почтовой связи. Просим Вас дать согласие на получение персональных данных от третьих лиц (п. 3 ст. 86 ТК РФ).

_____ _____ _____

С уведомлением ознакомлен(-а):

_____ _____ _____

Приложение №5
к настоящему Положению

СОГЛАСИЕ
на передачу персональных данных третьей стороне

Я, _____,
проживающий (– ая) по адресу_____
_____,
паспорт серии _____, номер _____, выдан_____
_____
«___»_____ _____ года,
ДАЮ СОГЛАСИЕ
ГКУ СК «Краевой центр информтехнологий», расположенному по адресу 355045, Ставропольский край, г. Ставрополь, ул. Пирогова, д. 18/6, на предоставление _____
_____
следующих моих персональных данных для _____
_____:

1. _____;
2. _____;
3. _____;
4. _____;
5. _____;

Настоящее согласие действительно в течение одного месяца с момента его получения.

«___»_____ 20__г. _____
(подпись)

Приложение №6
к настоящему Положению

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных
ГКУ СК «Краевой центр информтехнологий»

Я, _____,
проживающий (– ая) по адресу_____
_____,
паспорт серии _____, номер _____, выдан _____
_____
«___»_____ _____ года, понимаю, что получаю доступ к персональным данным в ГКУ СК «Краевой центр информтехнологий». Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных. Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный. В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными соблюдать все описанные в Положении о порядке обработки и защите персональных данных требования.

В случае попытки посторонних лиц получить от меня сведения, составляющие персональные данные субъектов, немедленно сообщу руководителю своего структурного подразделения.

В случае расторжения со мною трудового договора или контракта, я обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных, или их утраты я несу ответственность в соответствии с ст. 90 ТК РФ.

С Положением о порядке обработки и защите персональных данных ГКУ СК «Краевой центр информтехнологий» и гарантиях их защиты ознакомлен(а).

«___»_____ 20__г. _____
(подпись)

Приложение №7
к настоящему Положению

РАЗЪЯСНЕНИЯ
субъекту персональных данных юридических последствий
отказа предоставить свои персональные данные

В соответствие с принципами обработки персональных данных, установленными Федеральным Законом от 27.06.2006 № 152-ФЗ «О персональных данных», при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, и актуальность по отношению к заявленным целям обработки персональных данных.

Кроме того, Оператор должен принимать необходимые меры по уточнению неполных или неточных персональных данных.

В случае, если субъект персональных данных отказывается предоставить свои персональные данные, либо представленные персональные данные являются неточными и (или) неполными по отношению к заявленным целям обработки персональных данных, ГКУ СК «Краевой центр информтехнологий» оставляет за собой право отказать в предоставлении своих услуг субъекту персональных данных.

Если ГКУ СК «Краевой центр информтехнологий» выявит факт умышленного представления субъектом неверных персональных данных, то ГКУ СК «Краевой центр информтехнологий» может потребовать с субъекта персональных данных возмещения соответствующих затрат.

«_____»_____ 20__г.

_____ _____ _____

Приложение №8
к настоящему Положению

Дополнительное соглашение № _____
к договору от «___» _____ 20___ года № _____

Ставрополь «___»_____ 20___ года

Государственное казенное учреждение Ставропольского края «Краевой центр информационных технологий», в лице _____, _____действующего на основании Устава, именуемое в дальнейшем «Заказчик» с одной стороны, и _____ _____ в лице _____ _____, действующего на основании _____, именуемое в дальнейшем «Исполнитель», с другой стороны, совместно именуемые «Стороны», заключили настоящее дополнительное соглашение о нижеследующем: дополнить договор от «____» _____ 20___ года № _____ разделом следующего содержания:

Конфиденциальность и безопасность персональных данных.

1. Вся предоставляемая Сторонами друг другу информация считается конфиденциальной и не подлежит разглашению третьим лицам.

2. Исполнитель обязуется осуществлять обработку персональных данных субъекта Заказчика в соответствии с принципами и правилами обработки персональных данных, предусмотренных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3. Цель обработки персональных данных субъекта Заказчика:_____ _____ _____ _____.

4. Перечень действий (операций) по обработке персональных данных, которые будут совершаться лицом, осуществляющим обработку персональных данных, в рамках поручения:_____ _____ _____ _____.

5. Исполнитель вправе осуществлять обработку следующих персональных данных субъекта Заказчика: _____ _____

6. Исполнитель обязуется соблюдать конфиденциальность полученных персональных данных субъекта Заказчика и обеспечить безопасность персональных данных при их обработке.

7. Исполнитель при обработке персональных данных субъекта Заказчика обязуется принимать все необходимые организационные, технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных.

8. Исполнитель обязуется обеспечивать безопасность персональных данных применением таких мер как: определение угроз безопасности персональных данных при их обработке в информационных системах; учёт машинных носителей персональных данных; обнаружение фактов несанкционированного доступа к персональным данным и принятием мер; контроль принимаемых мер по обеспечению безопасности персональных данных и уровня защищённости информационных систем персональных данных; и другие меры.

9. Стороны принимают все необходимые меры для того, чтобы предотвратить разглашение получаемой информации в рамках настоящего договора. Информация может быть предоставлена

третьим лицам только в порядке, установленным действующим законодательством Российской Федерации.

10.Настоящее дополнительное соглашение является неотъемлемой частью договора от «___» _____ 20___ года № _____, составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

11.Дополнительное соглашение вступает в силу с момента подписания настоящего соглашения Сторонами.

ГКУ СК
«Краевой центр информтехнологий»
Юридический адрес:
355045, г. Ставрополь, ул. Пирогова, 18/6
Фактическое местонахождение:
355045, г. Ставрополь, ул. Пирогова, 18/6
ИНН 2635805516, **КПП** 263501001
р/с 40201810800000100001
ГРКЦ ГУ Банка России по Ставропольскому краю

Директор

_____

Приложение№ 9
к настоящему Положению

«УТВЕРЖДАЮ»
Директор ГКУ СК
"Краевой центр информтехнологий"
_____
«____» _____ 20___ г.

АКТ № _____
уничтожения персональных данных субъектов

Комиссия государственного казенного учреждения Ставропольского края «Краевой центр информационных технологий» произвела отбор к уничтожению персональных данных:

№ п/п	Тип носителя	Регистрационный номер носителя/наименование ИСПДн	Дата регистрации	Количество листов/файлов/полей

Причина уничтожения: _____
_____
(достижение целей обработки, решение субъекта ПДн, недостоверные ПДн и т.д.)

Всего подлежит уничтожению __ (_____) наименований документов.
(цифрами) (прописью)

 ПДн, размещенные на бумажных носителях уничтожены путём измельчения в устройстве для измельчения бумаги.

 ПДн, размещенные в ИСПДн уничтожены путем затирания информации в базах данных ИСПДн.

 ПДн, размещенные на физических носителях уничтожены путем удаления файлов с носителя (форматировании носителя).

 ПДн, размещенные на физических носителях уничтожены путем полного нарушения работоспособности носителя.

Председатель комиссии _____ _____

Члены комиссии _____ _____
_____ _____