

**ГЛАВА
КАМСКО-УСТЬИНСКОГО
МУНИЦИПАЛЬНОГО
РАЙОНА
РЕСПУБЛИКИ ТАТАРСТАН**



**ТАТАРСТАН
РЕСПУБЛИКАСЫ
КАМА ТАМАГЫ
МУНИЦИПАЛЬ РАЙОНЫ
БАШЛЫГЫ**

ул. Калинина, д.31,
пгт. Камское Устье, 422820

Калинин урамы, 31 йорт,
штп. Кама Тамагы, 422820

тел.: (884377) 2-11-51, факс: 2-18-86, e-mail: Kamuste.Sekretar@tatar.ru, <http://kamskoye-ustye.tatarstan.ru>.

РАСПОРЯЖЕНИЕ

от 24.05.2021 г.

БОЕРЫК

№ 9

О мерах, направленных на реализацию требований постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»

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

1. Назначить ответственным за организацию обработки персональных данных заместителя Главы Камско-Устьинского муниципального района Республики Татарстан Габидуллина Г.А.

2. Утвердить:

Правила обработки персональных данных в аппарате Совета Камско-Устьинского муниципального района Республики Татарстан согласно приложению № 1 к настоящему распоряжению;

Правила рассмотрения запросов субъектов персональных данных или их представителей согласно приложению № 2 к настоящему распоряжению;

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в аппарате Совета Камско-Устьинского муниципального района Республики Татарстан согласно приложению № 3 к настоящему распоряжению;

Правила работы с обезличенными данными в аппарате Совета Камско-Устьинского муниципального района Республики Татарстан в случае обезличивания персональных данных согласно приложению № 4 к настоящему распоряжению;

Перечень информационных систем персональных данных аппарата Совета Камско-Устьинского муниципального района Республики Татарстан согласно приложению № 5 к настоящему распоряжению;

Перечень персональных данных, обрабатываемых в аппарате Совета Камско-Устьинского муниципального района Республики Татарстан в связи с реализацией служебных или трудовых отношений согласно приложению № 6 к настоящему распоряжению;

Перечень персональных данных, обрабатываемых в аппарате Совета Камско-Устьинского муниципального района Республики Татарстан в связи с оказанием государственных и муниципальных услуг и осуществлением государственных функций согласно приложению № 7 к настоящему распоряжению;

Перечень должностей служащих аппарата Совета Камско-Устьинского муниципального района Республики Татарстан, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных согласно приложению № 8 к настоящему распоряжению;

Перечень должностей служащих аппарата Совета Камско-Устьинского муниципального района Республики Татарстан, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным согласно приложению № 9 к настоящему распоряжению;

Должностную инструкцию ответственного за организацию обработки персональных данных в аппарате Совета Камско-Устьинского муниципального района Республики Татарстан согласно приложению № 10 к настоящему распоряжению;

Типовое обязательство служащего аппарата Совета Камско-Устьинского муниципального района, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей согласно приложению № 11 к настоящему распоряжению;

Типовую форму согласия на обработку персональных данных служащих аппарата Совета Камско-Устьинского муниципального района, иных субъектов персональных данных согласно приложению № 12 к настоящему распоряжению;

Порядок доступа служащих аппарата Совета Камско-Устьинского муниципального района в помещения, в которых ведётся обработка персональных данных согласно приложению № 13 к настоящему распоряжению.

3. Ответственному за организацию обработки персональных данных:

- 1) организовать сбор обязательств служащих аппарата Совета Камско-Устьинского муниципального района прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей в случае расторжения с ними служебного контракта. Ознакомить служащих аппарата Совета Камско-Устьинского муниципального района, участвующих в обеспечении сбора указанных обязательств служащих аппарата Совета Камско-Устьинского муниципального района с настоящим распоряжением;
 - 2) организовать хранение обязательств служащих аппарата Совета Камско-Устьинского муниципального района прекратить обработку персональных данных, ставших известными им в связи с исполнением должностных обязанностей в случае расторжения с ними служебного контракта в личных делах указанных служащих;
 - 3) организовать сбор согласия служащих, иных субъектов персональных данных аппарата Совета Камско-Устьинского муниципального района на обработку персональных данных, указанного в приложении № 12 к настоящему распоряжению. Ознакомить служащих аппарата Совета Камско-Устьинского муниципального района, участвующих в обеспечении сбора согласий на обработку персональных данных служащих аппарата Совета Камско-Устьинского муниципального района с настоящим распоряжением;
 - 4) организовать хранение согласий на обработку персональных данных служащих аппарата Совета Камско-Устьинского муниципального района в личных делах указанных служащих.
4. Контроль исполнения настоящего распоряжения оставляю за собой.

Н.А. Вазыхов

Приложение № 1
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПРАВИЛА **обработки персональных данных в аппарате Совета Камско-Устьинского** **муниципального района Республики Татарстан**

1. Основные понятия

В настоящем документе используются следующие основные понятия:

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

безопасность персональных данных – состояние защищенности персональных данных, характеризующееся способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных;

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

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

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных 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 назначению и техническим характеристикам;

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;

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

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

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

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

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (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;

трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

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

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

2. Общие положения

Настоящие Правила обработки персональных данных (далее – Правила) разработаны для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных аппарата Совета Камско-Устьинского муниципального района Республики Татарстан (далее – Совет), а также защиты прав и свобод граждан при обработке их персональных данных в Совете, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также разъяснение ответственности должностных лиц (служащих), имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящие Правила устанавливают порядок обработки персональных данных субъектов персональных данных в Совете и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере персональных данных.

Субъектами персональных данных в Совете являются:

Под обработкой персональных данных понимается 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.

Настоящие Правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Обработке подлежат только те персональные данные, которые отвечают целям их обработки и не должны быть избыточными по отношению к заявленным целям.

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.

В случаях, предусмотренных действующим законодательством, сведения о доходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей могут размещаться на официальном сайте Камско-Устьинского муниципального района Республики Татарстан или предоставляться региональным средствам массовой информации по их запросам для последующего опубликования.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей персональных данных определяют законодательство Российской Федерации об обработке и защите персональных данных, а также действующие нормативные правовые акты Совета.

Совет является оператором персональных данных субъектов, указанных в настоящем документе. На основании соглашения (договора) Совета может поручать обработку персональных данных третьим лицам с согласия субъекта персональных данных, 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 (далее - поручение Совета). Лицо, осуществляющее обработку персональных данных по поручению Совета, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении Совета, 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 № 152-ФЗ.

Лицо, осуществляющее обработку персональных данных по поручению Совета, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

В случаях, когда Совет поручает обработку персональных данных третьему лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Совет. Лицо, осуществляющее обработку персональных данных по поручению Совета, несет ответственность перед Советом.

Совет 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.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации, Совет вправе получать и обрабатывать данные о частной жизни гражданских служащих и(или) работников Совета только с их письменного согласия.

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

Совет не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами обработки персональных данных.

Все изменения в Правила вносятся распоряжением Совета.

3. Правила обработки персональных данных

Все персональные данные субъектов Совета получает от них самих либо от их законных представителей.

Персональные данные ближайших родственников работников (служащих), необходимые для ведения кадрового учёта, Совет получает от самих работников.

Обработка персональных данных осуществляется на законной и справедливой основе, а также с соблюдением принципов и правил, предусмотренных Федеральным законом № 152-ФЗ на основании согласия субъекта персональных данных на обработку его персональных данных, кроме случаев, предусмотренных Федеральным законом № 152-ФЗ. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например, анкеты, бланки).

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

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных Совет вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152-ФЗ.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются Советом.

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

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.

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

При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц возможно только при предварительном уведомлении субъекта и с его письменного согласия. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

Персональные данные могут быть получены Советом от лица, не являющегося субъектом персональных данных, при условии предоставления Советом подтверждения наличия оснований, указанных в Федеральном законе № 152-ФЗ.

Персональные данные субъектов Совета обрабатываются в структурных подразделениях в соответствии с исполняемыми ими функциями и обязанностями.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком допущенных лиц, утверждённом в порядке, определяемом в Совете.

Доступ к персональным данным, обрабатываемым в информационных системах персональных данных, осуществляется в соответствии со списком допущенных лиц, утверждённом в порядке, определяемом в Совете.

Уполномоченные лица, допущенные к персональным данным субъектов Совета, имеют право получать только те персональные данные субъекта, которые

необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями (обязанностями) указанных лиц.

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» утвержденного Постановлением Правительства РФ от 15 сентября 2008 № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

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

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются распоряжением об утверждении мест хранения материальных носителей персональных данных Совета.

Персональные данные могут подлежать блокированию, уточнению, уничтожению либо обезличиванию в одном из следующих случаев:

- 1) выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных;
- 2) 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;
- 3) выявления неправомерной обработки персональных данных, осуществляемой Советом или лицом, действующим по поручению Совета и невозможности обеспечить правомерную обработку персональных данных;
- 4) достижения целей обработки или в случае утраты необходимости в их достижении;
- 5) отзыва согласия субъекта персональных данных на обработку его персональных данных;
- 6) представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными, неактуальными (устаревшими), незаконно полученными или не являются необходимыми для заявленной цели обработки.

В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных Совет осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) с момента такого обращения или получения указанного запроса на период проверки.

В случае выявления неточных персональных данных при обращении субъекта персональных данных или его законного представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Совет осуществляет блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных Совета на основании сведений, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов уточняет персональные данные либо обеспечивает их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) в течение 7 рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

В случае выявления неправомерной обработки персональных данных, осуществляемой Советом или лицом, действующим по поручению Совета, Совет в срок, не превышающий 3-х рабочих дней с даты этого выявления, осуществляет прекращение неправомерной обработки персональных данных или обеспечивает прекращение неправомерной обработки персональных данных лицом, действующим по поручению Совета.

В случае, если обеспечить правомерность обработки персональных данных невозможно, Совет в срок, не превышающий 10 рабочих дней с даты выявления неправомерной обработки персональных данных, осуществляет уничтожение таких персональных данных или обеспечивает их уничтожение. Решение о неправомерности обработки персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до руководства. Об устранении допущенных нарушений или об уничтожении персональных данных Совет уведомляет субъекта персональных данных или его законного представителя, а в случае, если обращение субъекта персональных данных или его законного представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

В случае достижения цели обработки персональных данных Совет прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) в срок, не превышающий 30 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 оператором и субъектом персональных данных либо если Советом не вправе осуществлять обработку

персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Советом прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) в срок, не превышающий 30 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 Советом и субъектом персональных данных либо если Совет не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или другими федеральными законами.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Совет вносит в них необходимые изменения.

В срок, не превышающий 7 рабочих дней со дня представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Совет уничтожает такие персональные данные. При этом Совет уведомляет субъекта персональных данных или его законного представителя о внесенных изменениях и принятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

В случае отсутствия возможности уничтожения персональных данных в течение срока, указанные выше по тексту, Совет осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Совета) и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

Уничтожение персональных данных осуществляет комиссия в составе руководителя и работников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) химическая обработка.

При этом составляется «Акт уничтожения документов Совета, содержащих персональные данные субъекта». Форма акта утверждается отдельным распоряжением.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Совета должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных Совета, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, работники структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется «Акт уничтожения полей баз данных Совета, содержащих персональные данные субъекта». Форма акта утверждается отдельным распоряжением.

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

При невозможности осуществления уничтожения информации в базах данных или на носителях, допускается проведение обезличивания путём перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была не возможна.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных в Совете.

Особенности обработки специальных категорий персональных данных, а также сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные), установлены соответственно статьями 10 и 11 Федерального закона № 152-ФЗ.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 Федерального закона № 152-ФЗ. Обработка персональных данных о судимости может осуществляться государственными органами или муниципальными органами в пределах полномочий, предоставленных им в соответствии с законодательством Российской

Федерации, а также иными лицами в случаях и в порядке, которые определяются в соответствии с федеральными законами.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 11 Федерального закона № 152-ФЗ.

Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

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.

Работники (служащие) Совета должны быть ознакомлены под роспись с требованиями законодательства Российской Федерации, касающимися обработки персональных данных, настоящими Правилами и другими документами Совета, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

4. Передача персональных данных третьим лицам

При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152;

2) предупреждать лиц, получающих персональные данные субъекта, 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 персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Совет запрашивает согласие субъекта в письменной форме. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовой формой документов, содержащих персональные данные субъекта (например: анкеты). Допускается совмещение формы согласия субъекта с другими формами согласий.

5. Права субъектов персональных данных

В целях обеспечения своих законных интересов субъекты персональных данных или его представители имеют право:

- 1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- 2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ;
- 3) требовать уточнение его персональных данных, их блокирование или уничтожение в случаях, 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. Субъект персональных данных при отказе Совета исключить или исправить, заблокировать или уничтожить его персональные данные имеет право заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;
- 4) требовать от Совета уведомления всех лиц, которым ранее были сообщены неверные или неполные, устаревшие, неточные, незаконно полученные или не являющиеся необходимыми для заявленной цели обработки персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них, в том числе блокирование или уничтожение этих данных третьими лицами;
- 5) обжаловать в суде или в уполномоченном органе по защите прав субъектов персональных данных любые неправомерные действия или бездействие Совета при обработке и защите персональных данных субъекта персональных данных, если субъект персональных данных считает, что Совет осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы.

В случае, если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Совет или направить ему повторный запрос в целях получения сведений, и ознакомления с персональными данными 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, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно до истечения 30 дневного срока в случае, если сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос должен содержать обоснование направления повторного запроса.

Совет вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренные частями 4 и 5 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Совете.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами Российской Федерации.

6. Порядок действий в случае запросов надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152 Совет сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение 30 дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных в Совете при необходимости с привлечением работников (служащих) Совета.

В течение установленного законодательством срока ответственный за организацию обработки персональных данных в Совете подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

7. Защита персональных данных субъекта

Защиту персональных данных субъектов от неправомерного их использования или утраты Совет обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) руководящим документом ФСТЭК России – «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) руководящим документом ФСТЭК России – «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Утверждены приказом ФСТЭК России № 17 от 11 февраля 2013 года;

3) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

4) внутренними документами Совета, действующими в сфере обеспечения информационной безопасности.

Защита персональных данных предусматривает ограничение к ним доступа.

Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются распоряжением Совета.

Руководитель структурного подразделения Совета, осуществляющего обработку персональных данных:

- 1) несёт ответственность за организацию защиты персональных данных в структурном подразделении;
 - 2) закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций и задач;
 - 3) организует изучение подчинёнными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;
 - 4) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении (отделе);
 - 5) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями работников подразделения.
- Работники (служащие), допущенные к персональным данным дают письменное обязательство о неразглашении таких данных.

8. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

- 1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Совета по обработке и защите персональных данных;
- 2) сохранять конфиденциальность персональных данных;
- 3) обеспечивать сохранность закреплённых за ними носителей персональных данных;
- 4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;
- 5) докладывать своему непосредственному руководителю структурного подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

Ответственный за организацию обработки персональных данных Совет организует проведение инструктажа и ознакомление работников Совета, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

9. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных субъектов

Лица, виновные в нарушении норм, регулирующих получение, обработку, передачу и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на

основании судебного решения, а также к дисциплинарной ответственности с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) предупреждение о неполном должностном соответствии;
- 4) освобождение или отстранение от занимаемой должности;
- 5) увольнение с гражданской службы.

Приложение № 2
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПРАВИЛА **рассмотрения запросов субъектов персональных данных** **или их представителей**

При устном обращении либо письменном запросе субъекта персональных данных или его законного представителя на доступ к персональным данным субъекта, Совет руководствуется требованиями статей 14, 18 и 20 Федерального закона Российской Федерации от 27 июля 2006 года № 152 «О персональных данных» (далее – Федеральный закон № 152-ФЗ).

Доступ субъекта персональных данных или его законного представителя к персональным данным субъекта Совета предоставляется только под контролем ответственного за организацию обработки персональных в аппарате Совета.

Обращение субъекта персональных данных или его законного представителя фиксируется в журнале регистрации обращений граждан на доступ к своим персональным данным. Рекомендуемая форма журнала приведена в приложении № 1.

Запрос субъекта персональных данных или его законного представителя фиксируется в журнале регистрации запросов граждан на доступ к своим персональным данным. Рекомендуемая форма журнала приведена в приложении № 2.

Ответственный за организацию обработки персональных данных принимает решение о предоставлении доступа субъекту персональных данных или его законному представителю к персональным данным указанного субъекта.

В случае, если данные предоставленные субъектом или его законным представителем не достаточны для установления его личности или предоставление персональных данных нарушают конституционные права и свободы других лиц, ответственный за организацию обработки персональных данных подготавливает мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 рабочих дней со дня обращения субъекта персональных данных или его законного представителя либо от даты получения запроса субъекта персональных данных или его законного представителя.

Для предоставления доступа субъекта персональных данных или его законного представителя к персональным данным субъекта ответственный за организацию обработки персональных данных привлекает работника (работников) структурного подразделения (отдела), обрабатывающего персональные данные субъекта по согласованию с руководителем этого структурного подразделения (отдела).

Совет предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Совет осуществляет в них необходимые изменения. В срок, не превышающий 7 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, Совет уничтожает такие персональные данные. Совет уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

Сведения о наличии персональных данных Совет предоставляет субъекту персональных данных или его законному представителю в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных. Контроль предоставления сведений субъекту или его законному представителю осуществляет ответственный за организацию обработки персональных данных.

Сведения о наличии персональных данных должны быть предоставлены субъекту персональных данных или его законному представителю при ответе на запрос в течение 30 дней от даты получения запроса субъекта персональных данных или его законного представителя.

Приложение №1
к приложению № 2
утверждённому распоряжением
Главы Камско-Устьинского
муниципального района
от 24.05.2021 № 9

Совет Камско-Устьинского муниципального района Республики Татарстан

**ЖУРНАЛ
регистрации обращений граждан на доступ к своим персональным данным**

Журнал начат « ____ » _____ 20__ года

Журнал завершён « ____ » _____ 20__ года

_____ / _____ /

_____ / _____ /

На _____ листах

--	--	--	--	--	--	--

Приложение № 2
к приложению № 2
утверждённому распоряжением
Главы Камско-Устьинского
муниципального района
от 24.05.2021 № 9

Совет Камско-Устьинского муниципального района Республики Татарстан

ЖУРНАЛ
регистрации запросов граждан на доступ к своим персональным данным

Журнал начат « ____ » _____ 20__ года

Журнал завершён « ____ » _____ 20__ года

_____ / _____ /

_____ / _____ /

На _____ листах

--	--	--	--	--	--	--	--

Приложение № 3
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленные Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами в Совете

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Совета.

Правила обязательны для исполнения всеми должностными лицами Совета, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Совета осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в Совете.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов Совета или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в Совете либо комиссией, образуемой Советом.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений Совета устанавливаются планом, утверждаемым руководителем Совета. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании распоряжения Совета. Ответственный за организацию обработки персональных данных в Совете подготавливает предложения по составу комиссии. Проект распоряжения о проверке подготавливает ответственный за организацию обработки персональных данных в Совете.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в структурное подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого структурного подразделения Совета, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

- 1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления работников проверяемого структурного подразделения со своей ответственностью;
- 2) получение при содействии работников проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;
- 3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом структурном подразделении Совета рассматриваются, в частности, следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных Совета, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Совете;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов работниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Совета работниками (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав работников, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных работников с данными документами;

ж) уровень подготовки работников, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);
 з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

- а) правильность отнесения обрабатываемой информации к персональным данным;
- б) правильность установления уровня защищенности персональных данных в информационной системе;
- в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях Совета, должностных инструкциях работников (служащих) и трудовых договорах;
- г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);
- д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;
- е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;
- ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;
- з) соответствие защищаемых помещений их техническим паспортам.

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

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

- 1) актом - при проведении проверки комиссией;
- 2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за организацию обработки персональных данных Совета. Второй экземпляр хранится в Совете в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок структурных подразделений периодически обобщаются ответственным за организацию обработки персональных данных в Совете и доводятся до руководителей структурных подразделений. При необходимости принятия решений по результатам проверок структурных подразделений на имя руководителя Совета готовятся соответствующие служебные записки.

Приложение № 4
к распоряжению
Исполнительного комитета
Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПРАВИЛА работы с обезличенными данными в Совете в случае обезличивания персональных данных

Настоящие правила разработаны в соответствии с положениями Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ) и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок работы с обезличенными данными в структурных подразделениях (отделах) Совета.

Правила обязательны для исполнения всеми должностными лицами Совета, допущенными к персональным данным.

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

Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор) как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации, установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, утверждены Методические рекомендации по применению приказа Роскомнадзора от 05.09.2013 года № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Методические рекомендации содержат анализ процессов автоматизированной обработки обезличенных данных, требования к обезличенным данным и методам обезличивания, позволяющей выделить основные свойства обезличенных данных и методов обезличивания и оценить возможность их применения при решении задач обработки персональных данных с учетом вида деятельности Оператора и необходимых действий с персональными данными.

К наиболее перспективным и удобным для практического применения относятся один из следующих методов обезличивания:

- 1) метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным);
- 2) метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);
- 3) метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим отдельным хранением подмножеств);
- 4) метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).

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

В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Совета исходя из служебной необходимости, и получение согласия субъекта на обработку его персональных данных не требуется на основании пункта 9 части 1 статьи 6 Федерального закона № 152-ФЗ.

Если обезличенные персональные данные используются в целях продвижения товаров, работ, услуг на рынке, или в целях политической агитации, Совет обязано получить согласие субъекта персональных данных на подобную обработку.

Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за организацию обработки персональных данных Совета для каждой информационной системы персональных данных индивидуально.

Приложение № 5
к распоряжению
Совета Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПЕРЕЧЕНЬ
информационных систем персональных данных Совета

№	Наименование ИСПДн	Категория ИСПДн	Уровень защищенности и персональных данных	Использование СКЗИ для обеспечения безопасности персональных данных
1	2	3	4	5
2	ГИС РТ Бухгалтерский учет и отчетность государственных органов Республики Татарстан и подведомственных им учреждений	ИСПДн-общедоступные	3 группа	Крипто Про CSP
3	1С: Предприятие	ИСПДн-общедоступные	3 группа	нет
4	СПО Документы ПУ - 6	ИСПДн-общедоступные	3 группа	нет

Приложение № 6
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в Совете в связи с реализацией
служебных или трудовых отношений

1. Фамилия, имя, отчество (последнее - при наличии) (в том числе прежние фамилии, имена и отчества (последнее - при наличии) в случае их изменения, сведения о том, когда, где и по какой причине они изменялись).
2. Дата рождения (число, месяц и год рождения).
3. Место рождения.
4. Вид, серия, номер основного документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи.
5. Реквизиты основного документа, удостоверяющего личность гражданина Российской Федерации, по которому гражданин Российской Федерации осуществляет выезд за пределы территории Российской Федерации и въезд на территорию Российской Федерации (серия, номер, когда и кем выдан).
6. Фотографии (размером 3x4 (6 штук) и размером 4x6 (6 штук), матовые, цветные, в овале).
7. Биометрические персональные данные.
8. Сведения о гражданстве (подданстве), в том числе прежнем, когда и по какой причине изменялось.
9. Адрес и дата регистрации по месту жительства (пребывания).
10. Адрес фактического проживания (нахождения).
11. Номера телефонов (домашнего, служебного, мобильного).
12. Почтовый адрес и адрес электронной почты.
13. Сведения о семейном положении, о составе семьи.
14. Сведения, содержащиеся в свидетельствах о государственной регистрации актов гражданского состояния.
15. Сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании, ученая степень, ученое звание (дата присвоения, реквизиты диплома, аттестата), иные сведения, содержащиеся в документе об образовании).
16. Сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке (повышении квалификации), квалификация и специальность по документу о

переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения.

17. Сведения о владении иностранными языками и языками народов Российской Федерации.

18. Сведения о выполняемой работе с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и другие).

19. Сведения о классном чине (квалификационном разряде) государственной службы Российской Федерации, муниципальной службы, дипломатическом ранге, воинском и (или) специальном звании, классном чине юстиции, классном чине прокурорских работников (кем и когда присвоены).

20. Сведения о родителях (в том числе усыновителях), детях (в том числе усыновленных и находящихся под опекой (попечительством), сестрах и братьях (полнородных и неполнородных), супругах (в том числе бывших) (степень родства, фамилия, имя, отчество (последнее - при наличии), дата рождения, место рождения, место работы (службы) и адрес регистрации по месту жительства (пребывания).

21. Сведения о форме и дате оформления допуска к государственной тайне, ранее имевшегося и (или) имеющегося.

22. Сведения о государственных наградах, иных наградах и знаках отличия (кем награжден(а) и когда).

23. Сведения о пребывании за границей (когда, где, с какой целью).

24. Сведения о родителях (в том числе усыновителях), детях (в том числе усыновленных), сестрах и братьях, (полнородных и неполнородных), а также супругах (в том числе бывших), постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество (последнее - при наличии), с какого времени проживают за границей).

25. Сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования.

26. Сведения, содержащиеся в свидетельстве о присвоении идентификационного номера налогоплательщика.

27. Сведения, содержащиеся в страховом медицинском полисе обязательного медицинского страхования.

28. Сведения, содержащиеся в документах воинского учета.

29. Сведения о наличии (отсутствии) судимости, в том числе снятой или погашенной.

30. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей (в том числе усыновленных и находящихся под опекой (попечительством).

31. Сведения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению.

32. Сведения о наличии (отсутствии) медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну.
33. Сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети "Интернет", на которых государственным гражданским служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации, размещались общедоступная информация, а также данные, позволяющие его идентифицировать.
34. Сведения об инвалидности, сроке действия установленной инвалидности.
35. Сведения, содержащиеся в уведомлении о намерении выполнять иную оплачиваемую работу.
36. Иные сведения, которые субъект персональных данных пожелал сообщить о себе.

Приложение № 7
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в Совете в связи с оказанием
государственных и муниципальных услуг и осуществлением
государственных функций

1. Фамилия, имя, отчество (последнее - при наличии) (в том числе прежние фамилии, имена и отчества (последнее - при наличии) в случае их изменения, сведения о том, когда, где и по какой причине они изменялись).
2. Дата рождения (число, месяц и год рождения).
3. Место рождения.
4. Вид, серия, номер основного документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи.
5. Реквизиты основного документа, удостоверяющего личность гражданина Российской Федерации, по которому гражданин Российской Федерации осуществляет выезд за пределы территории Российской Федерации и въезд на территорию Российской Федерации (серия, номер, когда и кем выдан).
6. Фотографии (размером 3x4 (6 штук) и размером 4x6 (6 штук), матовые, цветные, в овале).
7. Биометрические персональные данные.
8. Сведения о гражданстве (подданстве), в том числе прежнем, когда и по какой причине изменялось.
9. Адрес и дата регистрации по месту жительства (пребывания).
10. Адрес фактического проживания (нахождения).
11. Номера телефонов (домашнего, служебного, мобильного).
12. Почтовый адрес и адрес электронной почты.
13. Сведения о семейном положении, о составе семьи.
14. Сведения, содержащиеся в свидетельствах о государственной регистрации актов гражданского состояния.
15. Сведения об образовании (наименование образовательной и (или) иной организации, год окончания, уровень профессионального образования, реквизиты документов об образовании, направление подготовки, специальность и квалификация по документу об образовании, ученая степень, ученое звание (дата

присвоения, реквизиты диплома, аттестата), иные сведения, содержащиеся в документе об образовании.

16. Сведения о дополнительном профессиональном образовании (профессиональной переподготовке, повышении квалификации) (наименование образовательной и (или) научной организации, год окончания, реквизиты документа о переподготовке (повышении квалификации), квалификация и специальность по документу о переподготовке (повышении квалификации), наименование программы обучения, количество часов обучения).

17. Сведения о владении иностранными языками и языками народов Российской Федерации.

18. Сведения о выполняемой работе с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и другие).

19. Сведения о классном чине (квалификационном разряде) государственной службы Российской Федерации, муниципальной службы, дипломатическом ранге, воинском и (или) специальном звании, классном чине юстиции, классном чине прокурорских работников (кем и когда присвоены).

20. Сведения о родителях (в том числе усыновителях), детях (в том числе усыновленных и находящихся под опекой (попечительством), сестрах и братьях (полнородных и неполнородных), супругах (в том числе бывших) (степень родства, фамилия, имя, отчество (последнее - при наличии), дата рождения, место рождения, место работы (службы) и адрес регистрации по месту жительства (пребывания).

21. Сведения о форме и дате оформления допуска к государственной тайне, ранее имевшегося и (или) имеющегося.

22. Сведения о государственных наградах, иных наградах и знаках отличия (кем награжден(а) и когда).

23. Сведения о пребывании за границей (когда, где, с какой целью).

24. Сведения о родителях (в том числе усыновителях), детях (в том числе усыновленных), сестрах и братьях, (полнородных и неполнородных), а также супругах (в том числе бывших), постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество (последнее - при наличии), с какого времени проживают за границей).

25. Сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования.

26. Сведения, содержащиеся в свидетельстве о присвоении идентификационного номера налогоплательщика.

27. Сведения, содержащиеся в страховом медицинском полисе обязательного медицинского страхования.

28. Сведения, содержащиеся в документах воинского учета.

29. Сведения о наличии (отсутствии) судимости, в том числе снятой или погашенной.

30. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера, а также о доходах, расходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей (в том числе усыновленных и находящихся под опекой (попечительством)).
31. Сведения о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению.
32. Сведения о наличии (отсутствии) медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну.
33. Сведения об адресах сайтов и (или) страниц сайтов в информационно-телекоммуникационной сети "Интернет", на которых государственным гражданским служащим, гражданином Российской Федерации, претендующим на замещение должности государственной гражданской службы Российской Федерации, размещались общедоступная информация, а также данные, позволяющие его идентифицировать.
34. Сведения об инвалидности, сроке действия установленной инвалидности.
35. Сведения, содержащиеся в уведомлении о намерении выполнять иную оплачиваемую работу.
36. Иные сведения, которые субъект персональных данных пожелал сообщить о себе.

Приложение № 8
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПЕРЕЧЕНЬ
должностей служащих, ответственных за проведение
мероприятий по обезличиванию обрабатываемых
персональных данных, в случае обезличивания
персональных данных

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1.	Организационный отдел	Заместитель начальника отдела
2.	Отдел бухгалтерского учета и отчетности	Начальник отдела
3.	Отдел бухгалтерского учета и отчетности	Заместитель начальника отдела
4.	Общий отдел	Начальник отдела
5.	Общий отдел	Главный специалист
6.	Юридический отдел	Начальник отдела

Приложение № 9
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПЕРЕЧЕНЬ
должностей служащих Совета, замещение которых
предусматривает осуществление обработки персональных
данных либо осуществление доступа к персональным
данным

№ п/п	Структурное подразделение (отдел)	Должность служащего
1.	Отдел организационной работы	Начальник отдела
2.	Отдел организационной работы	Главный специалист
3.	Отдел опеки и попечительства	Главный специалист
4.	Отдел инфраструктурного развития	Главный специалист
5.	Отдел ЗАГС	Начальник отдела
6.	Отдел ЗАГС	Главный специалист
7.	Архивный отдел	Начальник отдела

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ответственного за организацию обработки персональных
данных в Совете

1. Общие положения

Ответственный за организацию обработки персональных данных (далее – Ответственный) является работником Совета.

Ответственный назначается распоряжением Совета.

Ответственный в вопросах организации обработки персональных данных подчиняется непосредственно руководителю Совета и проводит мероприятия по защите персональных данных в интересах Совета.

Ответственный в своей деятельности руководствуется:

- 1) Конституцией Российской Федерации;
- 2) Федеральными законами Российской Федерации и нормативными правовыми актами органов государственной власти по вопросам защиты персональных данных;
- 3) Государственными стандартами Российской Федерации в области защиты информации;
- 4) Руководящими и нормативными правовыми документами Федеральной Службы по техническому и экспортному контролю России;
- 5) Локальными нормативными актами Совета по защите персональных данных;
- 6) Правилами внутреннего трудового распорядка.

Деятельность Ответственного осуществляется согласно плану мероприятий по защите персональных данных Совета на год.

2. Задачи

На Ответственного возложены следующие задачи:

- 1) организация внутреннего контроля за соблюдением работниками (служащими) Совета норм законодательства Российской Федерации по обработке персональных данных, в том числе требований, предъявляемых к защите персональных данных;
- 2) разработка, внедрение и актуализация локальных актов по вопросам обработки персональных данных;
- 3) доведение до сведения работников (служащих) Совета, непосредственно осуществляющих обработку персональных данных, положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных, и проведение обучения указанных работников;
- 4) осуществление контроля приёма и обработки обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки

персональных данных и внесение предложений по организации приёма и обработки таких обращений и запросов;

5) осуществление рассмотрения обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и организация предоставления субъектам персональных данных или их законным представителям информации, предусмотренной Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

б) определение методов и способов проведения обезличивания персональных данных в информационных системах;

7) организация комплексной защиты объектов информатизации Совета, а именно:

а) информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих персональные данные субъектов Совета;

б) 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 персональные данные субъектов Совета.

8) организация защиты персональных данных субъектов Совета;

9) разработка и проведение организационных мероприятий, обеспечивающих безопасность объектов защиты Совета, своевременное выявление и устранение возможных каналов утечки информации;

10) организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Совета;

11) реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в структурных подразделениях (отделах) Совета;

12) методическое руководство системой обеспечения информационной безопасности Совета;

13) организация контроля состояния и проведение оценки эффективности системы обеспечения информационной безопасности персональных данных, а также реализация мер по её совершенствованию;

14) внедрение в информационную инфраструктуру Совета современных методов и средств обеспечения информационной безопасности.

3. Функции

Для решения поставленных задач Ответственный осуществляет следующие функции:

- 1) участие в разработке и внедрении правовых, организационных и технических мер по комплексному обеспечению безопасности персональных данных;
- 2) контроль обеспечения соблюдения режима конфиденциальности при обработке персональных данных и внесение предложений по соблюдению такого режима;
- 3) контроль выполнения мер по обезличиванию персональных данных в информационных системах при наступлении достижения целей обработки персональных данных или утраты необходимости в достижении этих целей, если ранее эти данные не были уничтожены;
- 4) разработка планов по защите персональных данных на объектах Совета;
- 5) контроль выполнения мер по защите персональных данных, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;
- 6) контроль выполнения плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите персональных данных, выполняемых контрагентами;
- 7) разработка и внесение предложений по обеспечению финансирования работ по защите персональных данных, в том числе выполняемых по договорам;
- 8) участие в проведении работ по технической защите информации на объектах информатизации Совета. Оценка эффективности принятых мер по технической защите информации;
- 9) внесение предложений по обеспечению выбора, установке, настройке и эксплуатации средств защиты информации в соответствии с организационно-распорядительной и эксплуатационной документацией;
- 10) контроль организации режима обеспечения безопасности помещений, в которых происходит обработка персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения, а также внесение предложений по обеспечению безопасности таких помещений;
- 11) участие в организации доступа работников (служащих) Совета к персональным данным в соответствии с возложенными на них должностными обязанностями и подготовка предложений по организации такого доступа;
- 12) разработка и внедрение локальных актов, определяющих перечень работников Совета, имеющих доступ к персональным данным;
- 13) контроль размещения устройств ввода (отображения) информации, исключающего её несанкционированный просмотр;
- 14) проведение оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения законодательства по защите персональных данных;
- 15) участие в разработке и реализации политики по работе с инцидентами информационной безопасности, в части обработки персональных данных;
- 16) внесение предложений по актуализации внутренней организационно-распорядительной документации по защите персональных данных при изменении

существующих и выходе новых нормативных правовых документов по вопросам обработки персональных данных и подготовка соответствующих необходимых проектов документов.

4. Права

Ответственный имеет право:

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

5. Взаимоотношения (служебные связи)

Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями (отделами) Совета.

Для выполнения своих функций и реализации предоставленных прав Ответственный взаимодействует с территориальными и региональными подразделениями

Федеральной службы по техническому и экспортному контролю России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации, Совет внутренних дел Российской Федерации и другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты персональных данных на законном основании.

6. Ответственность

Ответственный несёт ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации обработки персональных данных в Совете в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Приложение № 11
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
служащего Совета, непосредственно осуществляющего обработку
персональных данных, в случае расторжения с ним служебного
контракта (контракта) или трудового договора прекратить обработку
персональных данных, ставших известными ему в связи с исполнением
должностных обязанностей

Я, _____, проживающий(-ая)
по адресу, _____
паспорт серии _____, номер _____, выдан _____

«__» _____ года, работая в _____ должности
_____ в Совете, в период
настоящих трудовых отношений и в течение 5 лет после их окончания, в
соответствии с Федеральным законом Российской Федерации от 27 июля 2006
года № 152-ФЗ «О персональных данных», обязуюсь:

1) не раскрывать третьим лицам и не распространять персональные данные
субъектов Совета, полученные при исполнении мной должностных
обязанностей;

2) прекратить обработку персональных данных, ставших известными мне в
связи с исполнением должностных обязанностей, и передать все носители
персональных данных субъектов Совета (документы, накопители данных в
электронном виде, кино- и фото-негативы, позитивы, и прочее) Ответственному
за организацию обработки персональных данных Совета.

Я понимаю, что разглашение персональных данных субъектов Совета, может
нанести ущерб субъектам персональных данных.

Я предупреждён(а) о том, что в случае разглашения или утраты мною сведений,
относящихся к персональным данным субъектов Совета, я несу ответственность
в соответствии со статьей 90 Трудового Кодекса Российской Федерации и могу
быть привлечён(а) к материальной, гражданско-правовой, административной и
уголовной ответственности, в соответствии с действующим законодательством
Российской Федерации.

«__» _____ 20__ года

_____ (подпись)

_____ (инициалы, фамилия)

Приложение № 12
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

Глава Камско-Устьинского
муниципального района

СОГЛАСИЕ
на обработку персональных данных служащих Совета, иных
субъектов персональных данных

Я, _____, проживающий(-ая)
по адресу, _____
паспорт серии _____, номер _____, выдан _____

«__» _____ года, в соответствии с Федеральным законом
Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных
данных», даю согласие руководителю Совета, расположенному по адресу _____, на
обработку моих персональных данных, а именно:

<i>ФИО</i>	<i>Адрес</i>	<i>Образование</i>
<i>Дата рождения</i>	<i>Паспортные данные</i>	<i>Доходы</i>
<i>Место рождения</i>	<i>Семейное положение</i>	<i>Профессия</i>

и другие:

(перечислить дополнительные категории персональных данных)

В целях:

(указать цели обработки)

Перечень допустимых действий, осуществляемых с персональными данными:
*сбор, систематизация, накопление, хранение, уточнение (обновление,
изменение), использование, обезличивание, блокирование, уничтожение;*

Минцифра РТ может осуществлять *автоматизированную/ смешанную/
неавтоматизированную* обработку персональных данных без (с) применения
(ем) ЭВМ, без (с) передачи(ей) по внутренней сети и без (с) передачи(ей) по сети
интернет.

Согласие вступает в силу со дня его подписания и действует в течение
_____. Действие настоящего согласия прекращается досрочно в

случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов, содержащих персональные данные. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

« _____ » _____ 20 года

(подпись)

(инициалы, фамилия)

Приложение № 13
к распоряжению
Главы Камско-Устьинского
муниципального района
Республики Татарстан
от 24.05.2021 № 9

ПОРЯДОК
доступа служащих Совета в помещения, в которых ведётся
обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нестандартных ситуациях.

Объектами охраны Совета являются:

- 1) помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;
- 2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;
- 3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее – спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются работники Совета, не допущенные к обработке персональных данных и лица, не являющиеся работниками Совета.

К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут работники структурных подразделений, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

Контроль соблюдения требований настоящей инструкции обеспечивает работник, назначенный ответственным за организацию обработки персональных данных в Совете.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

Например, металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа работников, допущенных к обработке персональных данных.

При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведется обработка персональных данных лиц из числа работников Совета, не допущенных к обработке персональных данных.

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка персональных данных, должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Доступ работников в помещения, в которых ведется обработка персональных данных в нерабочее время, допускается по распоряжению руководства Совета.

3. Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведётся обработка персональных данных, осуществляется в соответствии со списком, утверждённым в Совете.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

Доступ в серверные помещения посторонних лиц допускается по согласованию с ответственным за обеспечение безопасности информационных систем персональных данных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных данных.

Доступ работников в серверные помещения в нерабочее время допускается по распоряжению руководства Совета.

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к средствам криптографической защиты информации (далее – СКЗИ). Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённым распоряжением Совета.

Доступ иных лиц в спецпомещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц их числа работников Совета.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Совета.

При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ работников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Совета.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.