

**«Политика Муниципального унитарного
предприятия г.Сочи «Городской
информационно-вычислительный центр»
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Утверждена приказом за №5-Р директора
МУП г. Сочи «ГорИВЦ»
«20» февраля 2013 года

ПОЛИТИКА
Муниципального унитарного предприятия «Городской информационно-вычислительный центр»
В ОТНОШЕНИИ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящая политика (далее - Политика) разработана в соответствии со ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о ПДн) и является основополагающим внутренним регулятивным документом муниципального унитарного предприятия «Городской информационно-вычислительный центр» (далее - Предприятие), определяющим ключевые направления его деятельности в области обработки и защиты персональных данных (далее - ПДн), оператором которых является Предприятие.

1.2. Политика разработана в целях реализации требований законодательства в области обработки и защиты ПДн и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его ПДн на Предприятии, в том числе защиты прав на неприкосновенность частной жизни, личной и семейной тайн.

1.3. Положения Политики распространяются на отношения по обработке и защите ПДн, полученных Предприятием как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и защите ПДн, полученных до ее утверждения.

1.4. Если в отношениях с Предприятием участвуют наследники (правопреемники) и (или) представители субъектов ПДн, то Предприятие становится оператором ПДн лиц, представляющих указанных субъектов. Положения Политики и другие внутренние регулятивные документы Предприятия распространяются на случаи обработки и защиты ПДн наследников (правопреемников) и (или) представителей субъектов ПДн, даже если эти лица во внутренних регулятивных документах прямо не упоминаются, но фактически участвуют в правоотношениях с Предприятием.

**2. Основания обработки и состав персональных данных,
обрабатываемых Предприятием**

2.1. Обработка ПДн Предприятием осуществляется в связи с выполнением функций, определяемых в соответствии с Уставом и заключаемыми договорами с юридическими лицами и индивидуальными предпринимателями – Поставщиками жилищно-коммунальных услуг по организации расчетов с потребителями.

Кроме того, обработка ПДн Предприятием осуществляется в ходе трудовых и иных непосредственно связанных с ними отношений, в которых Предприятие выступает в качестве работодателя (гл. 14 Трудового кодекса Российской Федерации), в связи с реализацией Предприятием своих прав и обязанностей как юридического лица.

2.2. В рамках осуществления функции по организации расчетов с потребителями ПДн обрабатываются Предприятием:

1) в ходе формирования печати и доставки единого платежного документа по оплате жилищно-коммунальных услуг;

2) в ходе оказания услуг по паспортно-учетной работе.

При этом обрабатываются ПДн:

а) потребителей жилищно-коммунальных услуг, которые учтены и переданы поставщиками жилищно-коммунальных услуг;

б) заявителей- получателей услуг по паспортно-учетной работе.

2.3. В связи с трудовыми и иными непосредственно связанными с ними отношениями, в которых Предприятие выступает в качестве работодателя, обрабатываются ПДн лиц, претендующих на трудоустройство на Предприятии, работников Предприятия (далее - Работники) и бывших Работников.

2.6. В связи с реализацией своих прав и обязанностей как юридического лица, Предприятием обрабатываются ПДн физических лиц, являющихся контрагентами (возможными контрагентами) Предприятия по гражданско-правовым договорам, ПДн руководителей, членов коллегиальных исполнительных органов и представителей юридических лиц, ПДн иных физических лиц, представленные участниками закупки, физических лиц, а также граждан, письменно обращающихся в Предприятие по вопросам его деятельности (помимо лиц, указанных в [пунктах 2.2](#) Политики).

2.9. ПДн получают и обрабатываются Предприятием на основании федеральных законов и иных нормативных правовых актов Российской Федерации, а в необходимых случаях - при наличии письменного согласия субъекта ПДн.

2.10. В целях исполнения возложенных на Предприятие функций Предприятие в установленном

порядке вправе поручить обработку ПДн третьим лицам.

В договоры с лицами, которым Предприятие поручает обработку ПДп, включаются условия, обязывающие таких лиц соблюдать предусмотренные законодательством требования к обработке и защите ПДн.

2.11. Предприятие предоставляет обрабатываемые им ПДн государственным органам и организациям, имеющим, в соответствии с федеральным законом, право на получение соответствующих ПДн.

2.12. Предприятием не производится обработка ПДн, несовместимая с целями их сбора. Если иное не предусмотрено федеральным законом, по окончании обработки ПДн Предприятием, в том числе при достижении целей их обработки или утраты необходимости в достижении этих целей, обрабатывавшиеся Предприятием ПДн уничтожаются или обезличиваются.

2.13. При обработке ПДн обеспечиваются их точность, достаточность, а при необходимости - и актуальность по отношению к целям обработки. Предприятие принимает необходимые меры по удалению или уточнению неполных или неточных ПДн.

3. Принципы обеспечения безопасности персональных данных

3.1. Основной задачей обеспечения безопасности ПДн при их обработке Предприятием является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения ПДн, разрушения (уничтожения) или искажения их в процессе обработки.

3.2. Для обеспечения безопасности ПДн Предприятие руководствуется следующими принципами:

1) законность: защита ПДн основывается на положениях нормативных правовых актов и методических документов уполномоченных государственных органов в области обработки и защиты ПДн;

2) системность: обработка ПДн Предприятием осуществляется с учетом всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн;

3) комплексность: защита ПДн строится с использованием функциональных возможностей информационных технологий, реализованных в информационных системах Предприятия (далее - ИС) и других имеющихся на Предприятии систем и средств защиты;

4) непрерывность: защита ПДн обеспечивается на всех этапах их обработки и во всех режимах функционирования систем обработки ПДн, в том числе при проведении ремонтных и регламентных работ;

5) своевременность: меры, обеспечивающие надлежащий уровень безопасности ПДн, принимаются до начала их обработки;

6) преемственность и непрерывность совершенствования: модернизация и наращивание мер и средств защиты ПДн осуществляется на основании результатов анализа практики обработки ПДн Предприятием с учетом выявления новых способов и средств реализации угроз безопасности ПДн, отечественного и зарубежного опыта в сфере защиты информации;

7) персональная ответственность: ответственность за обеспечение безопасности ПДн возлагается на Работников в пределах их обязанностей, связанных с обработкой и защитой ПДн;

8) минимизация прав доступа: доступ к ПДн предоставляется Работникам только в объеме, необходимом для выполнения их должностных обязанностей;

9) научная обоснованность и техническая реализуемость: уровень мер по защите ПДн определяется современным уровнем развития информационных технологий и средств защиты информации;

10) специализация и профессионализм: реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн осуществляются Работниками, имеющими необходимые для этого квалификацию и опыт;

11) эффективность процедур отбора кадров и выбора контрагентов: кадровая политика Предприятия предусматривает тщательный подбор персонала и мотивацию Работников, позволяющую исключить или минимизировать возможность нарушения ими безопасности ПДн; минимизация вероятности возникновения угрозы безопасности ПДн, источники которых связаны с человеческим фактором, обеспечивается получением наиболее полной информации о контрагентах Предприятия до заключения договоров;

12) наблюдаемость и прозрачность: меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результаты их применения были явно наблюдаемы (прозрачны) и могли быть оценены лицами, осуществляющими контроль;

13) непрерывность контроля и оценки: устанавливаются процедуры постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля регулярно анализируются.

4. Доступ к обрабатываемым персональным данным

4.1. Доступ к обрабатываемым Предприятием ПДн имеют лица, уполномоченные приказом Предприятия, лица, которым Предприятие поручило обработку ПДн на основании заключенного договора, а также лица, чьи ПДн подлежат обработке.

4.2. В целях разграничения полномочий при обработке ПДн полномочия по реализации каждой функции Предприятия закрепляются за соответствующими структурными подразделениями Предприятия.

Доступ к ПДн, обрабатываемым в ходе реализации полномочий, закрепленных за конкретным структурным подразделением Предприятия, могут иметь только Работники этого структурного подразделения. Работники допускаются к ПДн, связанным с деятельностью другого структурного подразделения, только для чтения и подготовки обобщенных материалов в части вопросов, касающихся структурного подразделения этих Работников.

4.3. Доступ Работников к обрабатываемым ПДн осуществляется в соответствии с их должностными обязанностями и требованиями внутренних регулятивных документов Предприятия.

Допущенные к обработке ПДн Работники под роспись знакомятся с документами Предприятия, устанавливающими порядок обработки ПДн, включая документы, устанавливающие права и обязанности конкретных Работников.

4.4. Порядок доступа субъекта ПДн к его ПДн, обрабатываемым Предприятием, определяется в соответствии с законодательством и определяется внутренними регулятивными документами Предприятия.

5. Реализуемые требования к защите персональных данных

5.1. Предприятие принимает правовые, организационные и технические меры (или обеспечивает их принятие), необходимые и достаточные для обеспечения исполнения обязанностей, предусмотренных Законом о ПДн и принятыми в соответствии с ним нормативными правовыми актами, для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

5.2. Состав указанных в [пункте 5.1](#) Политики мер, включая их содержание и выбор средств защиты ПДн, определяется, а внутренние регулятивные документы об обработке и защите ПДн утверждаются (издаются) Предприятием исходя из требований:

Закона о ПДн;

главы 14 Трудового кодекса Российской Федерации;

постановления Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

приказа ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн";

постановления Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

иных нормативных правовых актов Российской Федерации об обработке и защите ПДн.

5.3. В предусмотренных законодательством случаях обработка ПДн осуществляется Предприятием с согласия субъектов ПДн.

Предприятием производится устранение выявленных нарушений законодательства об обработке и защите ПДн.

5.4. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше чем этого требуют цели обработки ПДн, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

5.5. Предприятием осуществляется ознакомление работников Предприятия, непосредственно осуществляющих обработку ПДн, с положениями законодательства о ПДн, в том числе требованиями к защите ПДн, Политикой и иными внутренними регулятивными документами по вопросам обработки ПДн, и (или) обучение указанных работников по вопросам обработки и защиты ПДн.

5.6. При обработке ПДн с использованием средств автоматизации Предприятием, в частности, применяются следующие меры:

1) назначается Ответственный за организацию обработки ПДн, являющийся одним из заместителей директора Предприятия;

2) утверждаются (издаются) внутренние регулятивные документы по вопросам обработки и защиты ПДн, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

3) осуществляется внутренний контроль и (или) аудит соответствия обработки ПДн Закону о ПДн и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, Политике и внутренним регулятивным документам Предприятия;

4) проводится оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Закона о ПДн, определяется соотношение указанного вреда и принимаемых Предприятием мер, направленных на обеспечение исполнения обязанностей, предусмотренных Законом о ПДн.

5.7. Обеспечение безопасности ПДн Предприятием при их обработке в ИСПДн достигается путем:

1) определения угроз безопасности ПДн. Тип актуальных угроз безопасности ПДн и необходимый уровень защищенности ПДн определяются в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

2) определения в установленном порядке состава и содержания мер по обеспечению безопасности ПДн, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности Предприятием могут разрабатываться компенсирующие меры, направленные на нейтрализацию актуальных угроз безопасности ПДн. В этом случае в ходе разработки СЗПДн проводится обоснование применения компенсирующих мер для обеспечения безопасности ПДн;

3) применения организационных и технических мер по обеспечению безопасности ПДн, необходимых для выполнения требований к защите ПДн, обеспечивающих определенные уровни защищенности ПДн, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Предприятием, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности ПДн;

учет машинных носителей ПДн, обеспечение их сохранности;

обнаружение фактов несанкционированного доступа к ПДн и принятие соответствующих мер;

восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

установление правил доступа к обрабатываемым ПДн, а также обеспечение регистрации и учета действий, совершаемых с ПДн;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

контроль за принимаемыми мерами по обеспечению безопасности ПДн, уровня защищенности ИСПДн.

5.8. Обеспечение защиты ПДн Предприятием при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

1) обособления ПДн от иной информации;

2) недопущения фиксации на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;

3) использования отдельных материальных носителей для обработки каждой категории ПДн;

4) принятия мер по обеспечению отдельной обработки ПДн при несовместимости целей обработки ПДн, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн;

5) соблюдения требований:

к отдельной обработке зафиксированных на одном материальном носителе ПДн и информации, не относящейся к ПДн;

уточнению ПДн;

уничтожению или обезличиванию части ПДн;

использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них ПДн;

хранению ПДн, в том числе к обеспечению отдельного хранения ПДн (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку ПДн либо имеющих к ним доступ.