УТВЕРЖДАЮ

Генеральный директор

ОАО «Расчетный центр Урала»

_____ А.В.Короткова

«12» октября 2012 г

# ПОЛИТИКА

**обеспечения безопасности персональных данных**

**при их обработке в ОАО «Расчетный центр Урала»**

СОГЛАСОВАНО

Ответственный за обеспечение безопасности

Персональных данных при их обработке

В ИСПДн «Кадры» \ «Партнер-М»

_____ И. С. Клоцман

«12» октября 2012 г

г. Екатеринбург

2012 год

## 1. Общие положения

Политика обеспечения безопасности персональных данных при их обработке в ОАО «Расчетный центр Урала» (далее – Политика, Политика безопасности) применяется ко всем действиям с персональными данными, находящихся в ОАО «Расчетный центр Урала» (далее Организация).

Цель Политики состоит в доведении до сотрудников Организации, клиентов Организации и лиц, желающих воспользоваться продуктами и услугами Организации, необходимой информации о целях, способах и методах обработки персональных данных и требованиях к обеспечению их безопасности.

Организация оставляет за собой право вносить необходимые изменения в Политику при изменении действующего законодательства РФ и условий своей деятельности. Политика и все изменения к ней утверждаются и вводятся в действие Приказом по Организации.

Действующая редакция Политики доступна в сети Интернет на официальном сайте организации http://www.rcurala.ru/.

## 2. Правовые обоснования и цели обработки персональных данных

2.1. Политика разработана на основании:

Федеральных законов Российской Федерации:

- «О Федеральной службе безопасности» от 3 апреля 1995 г. № 40-ФЗ;
- «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ;
- «О персональных данных» от 27 июля 2006 г. № 152-ФЗ;
- «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ;

Указах Президента Российской Федерации:

- «Вопросы Федеральной службы безопасности Российской Федерации» от 11.08.2003 г. № 960;
- «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 № 351;

Постановлений Правительства Российской Федерации:

- «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного 17 ноября 2007 г. № 781;

Нормативных документах ФСБ, ФАПСИ:

- «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622;

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/5-144;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденное приказом ФСБ России от 9 февраля 2005 г. № 66;
- Приказа ФАПСИ «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» от 13 июня 2001 г. № 152;

2.2. Организация осуществляет обработку персональных данных в целях

- расчёта объема и стоимости потреблённых коммунальных услуг,
- учета поступившей оплаты за потребленные коммунальные услуги,
- расчета различного вида компенсаций различным категориям граждан;
- предоставление заинтересованным лицам (администрации Свердловской области, администрациям муниципальных образований, поставщикам коммунальных услуг, управляющим компаниям и т.д.) обобщенной статистической информации по расчёту стоимости и оплате ЖКУ;
- персонального учета сотрудников.

2.3. В отношении персональных данных осуществляются следующие действия: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача);

2.4. Требования Политики являются обязательными для пользователей локальной вычислительной сети (ЛВС) Организации, администраторов ЛВС, а также для иных должностных лиц, принимающих участие в подключении пользователей и сопровождении защищенных сетевых узлов в период эксплуатации информационных систем Организации.

## 3. Лица, имеющие доступ к персональным данным

К обрабатываемым персональным данным имеют доступ работники Организации, которые в соответствии с их должностными обязанностями наделены такими полномочиями. Доступ иных лиц к персональным данным, обрабатываемым организацией, может быть предоставлен исключительно в предусмотренных законом случаях, либо с согласия субъекта обрабатываемых персональных данных.

## 4. Реализуемые Организацией требования к защите персональных данных

Безопасность персональных данных при их обработке в информационных системах Организации осуществляется с помощью системы защиты информации, включающей организационные меры, средства защиты информации и средства криптографической защиты информации, средства защиты информации от несанкционированного доступа.

Защита персональных данных при их передачи по каналам связи осуществляется за счёт организационных мер, программно-аппаратных средств защиты информации.

Помещения, в которых размещены рабочие места работников Организации и технические средства (персональные компьютеры, средства коммутации), задействованные при обработке персональных данных, находятся под охраной, введенный режим безопасности обеспечивает постоянный контроль над пребыванием посторонних лиц в помещениях.

Обработка персональных данных в информационных системах Организации осуществляется при соблюдении условий:

- реализованы мероприятия по защите от несанкционированного доступа к персональным данным при их обработке в информационных системах Организации;
- реализованы мероприятия по защите информации от утечки по техническим каналам;
- реализованы мероприятия по обеспечению безопасности персональных данных с использованием шифровальных средств;
- реализованы регулярные мероприятия планирования работ по обеспечению безопасности персональных данных;
- реализованы мероприятия по резервированию и восстановлению работоспособности технических средств, общего и прикладного программного обеспечения и массивов персональных данных информационных систем Организации;

Во исполнение предписания ст.18.1. п.2 ФЗ-152 документ, определяющий политику оператора в отношении обработки персональных данных содержит только высокоуровневые правила и требования к данной деятельности в целях публикации на сайте Организации или размещения в помещениях Организации в свободном доступе.

## 5. Сроки обработки персональных данных

Сроки обработки персональных данных определяются исходя из целей обработки персональных данных, в соответствии с требованиями федеральных законов. А именно:

- Организация обязуется предоставить безвозмездно субъекту персональных данных или его уполномоченному представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его уполномоченным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его уполномоченным представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные.
- В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его уполномоченного представителя, либо по запросу субъекта персональных данных или его уполномоченного представителя, либо уполномоченного органа по защите прав субъектов персональных данных Организация обязуется осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его уполномоченного представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных Организация обязуется осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Организации) 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 Организация, на основании сведений, представленных субъектом персональных данных или его уполномоченным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязуется уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению

Организации) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

- В случае выявления неправомерной обработки персональных данных, осуществляемой Организацией или лицом, действующим по поручению Организации, Организация в срок, не превышающий трех рабочих дней с даты обнаружения факта неправомерной обработки ПД, обязуется прекратить неправомерную обработку ПД или обеспечить прекращение неправомерной обработки ПД лицом, действующим по поручению Организации. В случае, если обеспечить правомерность обработки персональных данных невозможно, Организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязуется уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Организация обязуется уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

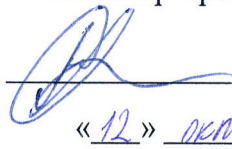
## 6. Ответственность

Лица, виновные в нарушении требований Федерального закона №152 о персональных данных, несут предусмотренную законодательством Российской Федерации ответственность.

Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом №152 о персональных данных, а также требований к защите персональных данных, установленных в соответствии с этим Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

РАЗРАБОТАНО

Инженер-программист УИТ



А. А. Аникин

«12» октября 2012 г