ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ АО «РЕГИОНАЛЬНЫЙ РАСЧЕТНО-КАССОВЫЙ ЦЕНТР»

г. Белгород 2010 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает применяемые в АО «Региональный расчетно-кассовый центр» (далее – РРКЦ) способы обеспечения безопасности при обработке, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, защиту, распространение (в том числе передачу), обезличивание, блокирование, уничтожение, персональных данных с целью соблюдения конфиденциальности сведений, содержащих персональные данные работников и физических лиц – абонентов (далее – абонентов).

1.2. Настоящее Положение разработано на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" и иных нормативных правовых актов Российской Федерации, а также локальных нормативных актов РРКЦ.

1.3. В соответствии с законодательством РФ под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация, необходимая РРКЦ в связи с трудовыми отношениями и осуществлением своей деятельности.

1.4. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами РРКЦ, допущенными к персональным данным, требования не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.5. Обеспечение конфиденциальности персональных данных не требуется в случае:
- обезличивания персональных данных;
- для общедоступных персональных данных.

1.6. Обработка и хранение конфиденциальных данных лицами, не имеющими допуска к персональным данным, запрещается.

1.7. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных РРКЦ предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:
- знакомит работника под роспись с требованиями «Положения о защите персональных данных работников АО «Региональный расчетно-кассовый центр», «Положения о защите персональных данных физических лиц-абонентов в Акционерном Обществе «Региональный расчетно-кассовый центр», с настоящим Положением, с должностной инструкцией и иными локальными нормативными актами РРКЦ в сфере обеспечения конфиденциальности и безопасности персональных данных;
- обеспечивают необходимые условия для хранения документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.);

- обучает правилам эксплуатации средств защиты информации;
- проводит иные необходимые мероприятия.

1.8. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.9. Должностные лица РРКЦ, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих должностных обязанностей обязанностей.

1.10. При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

1.11. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством РФ, в соответствии с «Положением о защите персональных данных работников АО «Региональный расчетно-кассовый центр», «Положением о защите персональных данных физических лиц- абонентов в Акционерном Обществе «Региональный расчетно-кассовый центр», с настоящим Положением, с должностной инструкцией и иными локальными нормативными актами РРКЦ в сфере обеспечения конфиденциальности и безопасности персональных данных.

1.12. Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта.

1.13. Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам.

1.14. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в РРКЦ локальными нормативными актами.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.15. Должностные лица РРКЦ, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) генеральному директору РРКЦ обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ, шкафов и др.), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

1.16. Отсутствие контроля со стороны РРКЦ за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством Российской Федерации ответственности.

2. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

2.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2.2. Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

- осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;
- информирует лиц, допущенных к обработке персональных данных, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления обработки без использования средств автоматизации;
- организует раздельное, т.е. не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

2.3. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, руководитель структурного подразделения, лица, ответственные за хранение персональных данных должны обеспечить раздельную обработку персональных данных, исключающую одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

2.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

3.1. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью информационных технологий и технических средств в информационных системах персональных данных РРКЦ (далее - ИС).

Безопасность персональных данных при их обработке в ИС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в ИС информационные технологии.

Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.2. Лица, допуск которых к персональным данным, обрабатываемым в ИС, необходим для выполнения должностных обязанностей, допускается к соответствующим персональным данным на основании приказа (или) списка, утвержденного генеральным директором РРКЦ при наличии ключей (паролей) доступа.

Работа с персональными данными, содержащимися в ИС, осуществляется в соответствии с требованиями «Положения о защите персональных данных работников АО «Региональный расчетно-кассовый центр», «Положения о защите персональных данных физических лиц- абонентов в Акционерном Обществе «Региональный расчетно-кассовый центр», с настоящим Положением, с должностной инструкцией и иными локальными нормативными актами РРКЦ в сфере обеспечения конфиденциальности и безопасности персональных данных с которыми работник, в должностные обязанности которого входит обработка персональных данных, знакомится под роспись.

3.3. Работа с персональными данными в ИС должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

3.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, в соответствии с «Парольной политикой АО «РРКЦ». Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.6. При обработке персональных данных в ИС пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

б) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в ИС разработчиками и администраторами систем должны обеспечиваться:
а) обучение лиц, использующих средства защиты информации, применяемые в ИС, правилам работы с ними;
б) учет лиц, допущенных к работе с персональными данными в ИС, прав и паролей доступа;
в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

4. ПОРЯДОК УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ТВЕРДЫМИ КОПИЯМИ И ИХ УТИЛИЗАЦИИ

4.1. Все находящиеся на хранении и в обращении в РРКЦ съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие персональные данные, подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь метку, на которой указывается его уникальный учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных осуществляет начальник отдела материально-технического обеспечения.

Работники РРКЦ получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок.

При получении делаются соответствующие записи в журнале персонального учета съемных носителей персональных данных (далее - журнал учета).

По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.3. При работе со съемными носителями, содержащими персональные данные, запрещается:
- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

4.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения и (или) генерального директора РРКЦ.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено руководителю соответствующего структурного подразделения и (или) генеральному директору РРКЦ.
На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета.

4.6. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, созданной приказом генерального директора РРКЦ.
По результатам уничтожения носителей составляется акт.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. С настоящим Положением должны быть ознакомлены под роспись все работники РРКЦ, имеющие отношение к обработке персональных данных.

5.2. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.