Небанковская кредитная организация
«Объединенная расчетная система»
(открытое акционерное общество)

УТВЕРЖДЕНА
Приказом Председателя Правления
НКО «ОРС» (ОАО)
от 20.03.2015 № 09

ПОЛИТИКА
обработки и обеспечения безопасности персональных данных в НКО «ОРС» (ОАО)

г. Москва

Оглавление

1. Общие положения

1.1. Целью настоящей Политики является исполнение предусмотренных законодательством Российской Федерации требований по обеспечению прав и свобод субъектов персональных данных при обработке их персональных данных в НКО «ОРС» (ОАО) (далее по тексту НКО), в том числе защита прав субъектов персональных данных на неприкосновенность частной жизни, личную и семейную тайну.

1.2. Настоящая Политика определяет цели обработки персональных данных, устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в НКО с использованием средств автоматизации или без использования таких средств.

1.3. Настоящая Политика разработана в соответствии с федеральным законодательством Российской Федерации.

1.4. Действие настоящей Политики распространяется на все внутренние структурные подразделения НКО.

1.5. Все работники НКО должны быть ознакомлены с настоящей Политикой под роспись.

1.6. Настоящая Политика является локальным нормативным актом НКО и вступает в силу с момента подписания Председателем Правления НКО или уполномоченным им лицом приказа о введении её в действие.

2. Основные термины

2.1. В настоящей Политике используются следующие термины:

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

НКО – НКО «ОРС» (ОАО);

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

документ (официальный) – документ, созданный НКО, а также юридическим или физическим лицом, оформленный (и/или удостоверенный) в установленном порядке;

доступ к информации, составляющей коммерческую тайну – ознакомление определенных лиц с информацией, составляющей коммерческую тайну НКО, с согласия НКО или на ином законном основании при условии сохранения конфиденциальности этой информации;

информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

коммерческая тайна – режим конфиденциальности информации, позволяющий НКО при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

контрагент – сторона гражданско-правового договора с НКО;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к информации, составляющей коммерческую тайну НКО, требование

не передавать такую информацию третьим лицам без согласия НКО, за исключением случаев, предусмотренных законодательством;

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным, получившим доступ к персональным данным лицом, требование не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

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

обладатель информации, составляющей коммерческую тайну – лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

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;

ответственный сотрудник НКО – специальное должностное лицо, назначаемое в соответствии с требованиями п. 2 ст. 7 Федерального Закона от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» приказом Председателя Правления НКО, ответственное за реализацию Правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма ПОД/ФТ);

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

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

разглашение информации, составляющей коммерческую тайну – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия НКО либо вопреки трудовому или гражданско-правовому договору;

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

режим коммерческой тайны – правовые, организационные, технические и иные принимаемые НКО в отношении информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

внутреннее структурное подразделение НКО – управление, отдел, служба;

субъект персональных данных (Субъект ПДн) – физическое лицо, к которому относятся персональные данные;

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

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.

2.2. В настоящем Положении используются следующие сокращения:

НСД – несанкционированный доступ.

3. Принципы и условия обработки персональных данных

3.1. Принципы обработки персональных данных в НКО

3.1.1. При обработке персональных данных должны выполняться следующие принципы:

- Обработка персональных данных должна осуществляться на законной и справедливой основе.
- Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- Обработке подлежат только персональные данные, которые отвечают целям их обработки.
- Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
- 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.
- Оператор ПДн должен принимать необходимые меры, по удалению или уточнению неполных или неточных данных.
- Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, должно осуществляться не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3.2. Способы обработки персональных данных

3.2.1. НКО может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

3.3. Конфиденциальность персональных данных

3.3.1. Работниками НКО, получившими доступ к персональным данным, обрабатываемым в НКО, должна быть обеспечена конфиденциальность таких данных.

3.3.2. Обеспечение конфиденциальности не требуется в отношении:

- обезличенных персональных данных;
- персональных данных, сделанных общедоступными субъектом персональных данных;
- персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.3.3. Персональные данные отнесены НКО к информации, составляющей коммерческую тайну, и включены в документально оформленный и утвержденный решением Правления НКО «Перечень сведений, составляющих коммерческую тайну НКО «ОРС» (ОАО)». Необходимый объем организационных мер, выполнение которых позволяет обеспечить конфиденциальность персональных данных в составе информации, составляющей коммерческую тайну, определен «Положением по обеспечению сохранности коммерческой тайны в НКО «ОРС» (ОАО)».

3.4. Передача персональных данных

3.4.1. НКО обрабатывает персональные данные сотрудников и клиентов самостоятельно, не поручая обработку персональных данных третьим лицам.

3.5. Общедоступные источники персональных данных

3.5.1. В целях информационного обеспечения в НКО могут создаваться общедоступные источники персональных данных (телефонный справочник, адресная книга и т.п.).

3.5.2. В состав справочников могут входить фамилия, имя, отчество, дата и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом.

3.5.3. НКО создаются общедоступные источники, содержащие персональные данные работников. Создание общедоступных источников персональных данных НКО осуществляется на основе письменного согласия субъекта, чьи персональные данные включаются в создаваемые общедоступные источники. Согласие работника на создание общедоступных источников собирается в составе документа заявление работника, подписываемого каждым работником НКО.

3.5.4. НКО раскрываются для неограниченного круга лиц в соответствии с федеральным законодательством с ведома и по письменному согласованию с субъектами персональных данных:

- сведения о работниках НКО, включаемые в Единый государственный реестр юридических лиц (ЕГРЮЛ) и являющиеся, в соответствии с Федеральным законом «О государственной регистрации юридических лиц и индивидуальных предпринимателей», открытыми и общедоступными;
- сведения, относящиеся к персональным данным и подлежащие обязательному раскрытию и опубликованию в соответствии с федеральными законами «Об акционерных обществах», «О банках и банковской деятельности», «О рынке ценных бумаг»;
- персональные данные членов Совета директоров, Правления и Ревизионной комиссии, публикуемые на сайте НКО.

3.5.5. Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

3.6. Принятие решений на основании исключительно автоматизированной обработки персональных данных

3.6.1. В НКО запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, перечисленных в п. 3.6.2.

3.6.2. 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 или в случаях, предусмотренных федеральными законами,

устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

Перед началом применения информационных систем для принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, НКО обязана:

- разъяснить субъекту персональных данных порядок принятия и возможные юридические последствия такого решения;
- разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов;
- получить в письменной форме согласие субъекта персональных данных на такой способ принятия решений при обработке его персональных данных.

После принятия на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, НКО обязана:

- известить субъекта о принятом решении с целью предоставления возможности заявить возражение против такого решения;
- рассмотреть возражение, поступившее от субъекта персональных данных, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

3.6.3. В соответствии со ст. 86 Трудового кодекса, при принятии решений, затрагивающих интересы работников, НКО как работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4. Субъекты и категории персональных данных

4.1. Категории субъектов персональных данных

4.1.1. НКО осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

Сотрудники НКО:

- работники – физические лица, связанные с НКО трудовыми отношениями, либо желающие вступить в такие отношения с НКО;
- контрагенты – физические лица, связанные с НКО отношениями гражданско – правового характера, либо желающие вступить в такие отношения с НКО;
- работники, с которыми расторгнуты трудовые договора, но сведения о которых НКО обязан хранить в соответствии с требованиям законодательства.

Субъекты других категорий:

- физические лица, отнесенные к аффилированным лицам;
- выгодоприобретатели – физические лица, к выгоде которых действует клиент, при проведении операций с денежными средствами и иным имуществом;
- бенефициарные владельцы - физические лица, которые, в конечном счете прямо или косвенно (через третьих лиц) владеют (имеют преобладающее участие более 10 процентов в капитале) клиентом - юридическим лицом либо имеют возможность контролировать действия клиента;
- представители юридических лиц – руководители, сотрудники, подписанты юридических лиц - клиентов, контрагентов и акционеров НКО, выступающие представителями ЮЛ при совершении операций и подписании договоров;
- представители клиентов – физические лица, являющиеся представителями клиентов НКО на основании доверенности, либо на основании Гражданского кодекса Российской Федерации;

- близкие родственники субъектов – физические лица, являющиеся родственниками работников НКО, данные которых фигурируют в анкетах и других документах субъекта;
- представители иностранной делегации – иностранные граждане, посещающие НКО в деловых и контрольных целях;
- представители контролирующих органов;
- посетители – физические лица, осуществляющие разовый проход на территорию НКО.

4.2. Согласие субъекта персональных данных на обработку своих персональных данных

4.2.1. Обработка персональных данных в информационных системах НКО должна осуществляться только с согласия субъекта персональных данных, за исключением случаев, приведенных в п. 4.2.7 настоящего Положения.

4.2.2. Письменное согласие субъекта необходимо получать:

- на обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояние здоровья, интимной жизни, если только сам субъект не сделал эти сведения общедоступными;
- при обработке биометрических[1] персональных данных;
- при включении персональных данных в общедоступные источники (справочники, адресные книги);
- в случаях трансграничной передачи персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных;
- при передаче обработки персональных данных другому лицу;
- при принятии на основании исключительно автоматизированной обработки персональных данных решения, порождающего юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы .

4.2.3. Согласие субъекта персональных данных может быть получено как в отдельном документе, так и в составе документа, на котором субъект персональных данных проставляет личную подпись.

4.2.4. Документом, в составе которого может быть получено согласие субъекта персональных данных на обработку своих персональных данных, является:

- разовый пропуск субъекта персональных данных на территорию НКО, предусматривающий поле, в котором субъект персональных данных может проставить отметку о согласии субъекта на обработку НКО его персональных данных;
- иной документ, содержащий отметку о согласии субъекта на обработку его персональных данных НКО.

4.2.5. Согласие субъекта персональных данных на обработку своих ПДн в письменной форме должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или

[1] Биометрические данные: физиологические – сетчатка глаза, отпечатки пальцев; поведенческие – голос, почерк

иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

- наименование и адрес НКО, как оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению НКО, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых НКО способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

4.2.6. Для обработки персональных данных, содержащихся в согласии, дополнительное согласие не требуется.

4.2.7. Согласие субъекта не требуется в случае, если:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на НКО функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необходима для осуществления прав и законных интересов НКО или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных, за исключением обработки персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;
- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее — персональные данные, сделанные общедоступными субъектом персональных данных);
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2.8. При запросе персональных данных, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора, одной из сторон которого является субъект персональных данных, в дополнение к данным, полученным НКО от субъекта в целях исполнения договора или требований законодательства, требуется получение согласия субъекта только на обработку дополнительно истребованных персональных данных НКО.

4.2.9. Согласие на обработку персональных данных, обработка которых не установлена требованиями законодательства или не требуется для исполнения договора, одной из сторон которого является субъект персональных данных, может быть отозвано субъектом персональных данных.

4.3. Категории персональных данных

4.3.1. В информационных системах НКО осуществляется обработка персональных данных следующих категорий:

- персональные данные сотрудников оператора (работников НКО);
- общедоступные персональные данные;
- иные категории персональных данных, за исключением специальных категорий персональных данных.

4.4. Специальные категории персональных данных

4.4.1. В НКО не подлежат обработке персональные данные, относящиеся к специальным категориям:

- расовая принадлежность;
- национальная принадлежность;
- политические взгляды;
- религиозные или философские убеждения;
- состояния здоровья, за исключением:
  - когда работник нуждается в переводе на другую работу в соответствии с медицинским заключением;
  - когда работник занят на работах с вредными и (или) опасными условиями труда, а также на работах, связанных с движением транспорта;
- интимная жизнь;
- персональные данные о частной жизни, о членстве субъектов персональных данных в общественных объединениях или их профсоюзной деятельности.

4.4.2. В случае принятия решения об обработке указанных категорий персональных данных, должно быть обеспечено выполнение одного из условий:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными.

4.4.3. Неавтоматизированная обработка персональных данных о судимости может осуществляться НКО в случаях и порядке, которые определяются соответствующими федеральными законами.

4.4.4. НКО осуществляет неавтоматизированную обработку данных о судимости работников, занимающих должности (претендующих на должности) членов Совета директоров (наблюдательного совета) НКО, руководителей НКО, Главного бухгалтера, заместителей главного бухгалтера НКО, Ответственного сотрудника НКО и сотрудников подразделения финансового мониторинга НКО, Начальников Служб внутреннего аудита, внутреннего контроля, управления рисками НКО, в соответствии с положениями Инструкции Центрального Банка Российской Федерации от 02.04.2010 № 135−И «О порядке принятия Банком России решения о государственной регистрации кредитных организаций и выдаче лицензий на осуществление банковских операций», принятой в соответствии с требованиями Федеральных законов «О банках и банковской деятельности», «Об акционерных обществах» от 26 декабря 1995 года N 208−ФЗ, «О

государственной регистрации юридических лиц и индивидуальных предпринимателей» от 8 августа 2001 года N 129−ФЗ, в соответствии с Указанием Банка России от 09.08.2004 №1486-У «О квалификационных требованиях к специальным должностным лицам, ответственным за соблюдение правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма и программ его осуществления в кредитных организациях», а также в соответствии с Указанием Банка России от 01.04.2014 № 3223-У «О требованиях к руководителям службы управления рисками, службы внутреннего контроля, службы внутреннего аудита кредитной организации».

4.5. Права субъектов персональных данных

4.5.1. В соответствии с действующим законодательством Российской Федерации НКО обязана обеспечить реализацию предусмотренных законодательством прав субъектов персональных данных. Субъект персональных данных вправе:

- получить сведения об НКО как операторе персональных данных, о месте ее нахождения, о наличии у НКО персональных данных, относящихся к этому субъекту персональных данных,
- ознакомиться со своими персональными данными, обрабатываемыми НКО;
- обжаловать действия или бездействие НКО в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- защищать свои права и законные интересы, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

4.5.2. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки НКО его персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые НКО способы обработки персональных данных;
- наименование и место нахождения НКО, сведения о лицах (за исключением работников НКО), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с НКО или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению НКО, если обработка поручена или будет поручена такому лицу;

4.5.3. Субъект персональных данных вправе требовать от НКО уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.5.4. Сведения о наличии персональных данных должны быть предоставлены представителем НКО субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4.6. Хранение персональных данных

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

цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные в соответствии с требованиями Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4.6.2. При определении сроков хранения персональных данных, помимо целей обработки ПДн, необходимо руководствоваться сроками исковой давности по гражданским делам (на основании Гражданского Кодекса), сроками хранения данных налогового учета (на основании налогового законодательства), установленными в Правилах внутреннего контроля в целях ПОД/ФТ сроками хранения со дня прекращения отношений с клиентом документов и сведений, представленных клиентом в результате проведения процедуры идентификации (на основании Федерального Закона от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»), приказом Министра культуры Российской Федерации от 25.08.2010 г. N 558 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения» и другими нормативными и законодательными актами Российской Федерации, устанавливающими сроки хранения (в том числе, архивного хранения) отдельных видов документов, содержащих персональные данные.

4.6.3. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном архивным законодательством Российской Федерации.

Персональные данные работников подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении таких целей.

4.6.4. Обезличивание персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей применяется только в случае необходимости хранения ПДн для обработки их в статистических или иных исследовательских целях (часть 9 статьи 6 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных»). С учетом установленных в Правилами внутреннего контроля в целях ПОД/ФТ сроков хранения идентифицирующих данных клиентов, необходимость обезличивания ПДн в НКО отсутствует.

5. Обязанности НКО при обработке персональных данных

5.1. Обязанности НКО при сборе персональных данных

5.1.1. Если обязанность предоставления персональных данных субъектом установлена федеральным законом, представитель НКО обязан разъяснить субъекту персональных данных юридические последствия отказа в предоставлении своих персональных данных.

5.1.2. Такими последствиями отказа в предоставлении своих персональных данных могут быть:

- для работника – отказ в заключение трудового договора с работодателем (для соискателей должностей), невозможность предоставления социальных льгот и дополнительных мер социальной защиты;
- для клиента – отказ в предоставлении (заказе) банковских услуг.

5.2. Организация обработки персональных данных

5.2.1. В соответствии с требованиями Федерального закона N 152-ФЗ «О персональных данных» в НКО назначается лицо, ответственное за организацию обработки персональных данных.

5.2.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от Председателя Правления и подотчетно ему.

5.2.3. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:

- осуществлять внутренний контроль за соблюдением НКО и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доводить до сведения работников НКО положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организовывать прием и обработку НКО обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

5.2.4. Руководители структурных подразделений обязаны оперативно предоставлять необходимые материалы и сведения по запросам лица, ответственного за организацию обработки персональных данных в НКО, а также устранять нарушения требований законодательства Российской Федерации при работе с персональными данными, в случае выявления их в подразделении.

5.3. Меры по обеспечению безопасности персональных данных при их обработке

5.3.1. НКО при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.3.2. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

5.3.3. В составе информационных систем персональных данных НКО должна применяться система, обеспечивающая защиту персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.3.4. Система защиты персональных данных реализуется организационными и техническими мерами и применением средств защиты информации.

5.4. Финансирование мероприятий по обеспечению безопасности персональных данных

5.4.1. Финансирование мероприятий по обеспечению безопасности персональных данных осуществляется за счет средств НКО.

5.5. Ответственность за нарушение требований законодательства

5.5.1. Лица, виновные в нарушении требований действующего федерального законодательства Российской Федерации в области персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность.

6. Мероприятия по обеспечению безопасности персональных данных

6.1. Общие положения

6.1.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности НКО.

6.1.2. Организация работ по обеспечению безопасности персональных данных осуществляется руководством НКО.

6.2. Обеспечение безопасности персональных данных при автоматизированной обработке

6.2.1. Безопасность персональных данных достигается путем исключения 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.

6.2.2. Безопасность персональных данных при их обработке в информационной системы персональных данных (ИСПДн) обеспечивается системой защиты персональных данных, включающей организационные и технические меры и средства защиты информации.

6.2.3. Лица, доступ которых к персональным данным, обрабатываемым в НКО, необходим для выполнения служебных (трудовых) обязанностей, допускаются к персональным данным на основании приказа (распоряжения) Председателя Правления.

6.2.4. Обязанности лиц, допускаемых к работе с персональными данными, определяются соответствующим разделом должностных инструкций.

6.3. Классификация информационных систем персональных данных

6.3.1. Все информационные системы персональных данных (далее – ИСПДн) НКО классифицируются по необходимому уровню защищенности комиссией, назначенной приказом Председателем Правления. Классификация по необходимому уровню защищенности осуществляется в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Результаты классификации по необходимому уровню защищенности оформляются актом, утверждаемым Председателем Правления.

6.4. Система защиты персональных данных

6.4.1. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные и технические меры и средства защиты информации. Выбор и реализация методов и способов защиты ПДн в информационной системе

осуществляется на основе класса по необходимому уровню защищенности ИСПДн и исходя из актуальных угроз безопасности персональных данных, определенных в соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

6.4.2. При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- возможность восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

6.4.3. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение и регламентация состава работников, имеющих доступ к персональным данным;
- ознакомление работников с требованиями федерального законодательства и нормативных документов НКО по обработке и защите персональных данных;
- обеспечение учёта и хранения материальных носителей информации и их обращения, исключающего хищение, подмену, несанкционированное копирование и уничтожение;
- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработку на основе модели угроз системы защиты персональных данных для соответствующего необходимого уровня защищенности;
- проверку готовности и эффективности использования средств защиты информации;
- реализацию разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;
- регистрацию и учёт действий пользователей информационных систем персональных данных;
- парольную защиту доступа пользователей к информационной системе персональных данных;
- применение средств контроля доступа к коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;
- применение в необходимых случаях средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи и хранении на машинных носителях информации;
- осуществление антивирусного контроля, предотвращение внедрения в корпоративную сеть вредоносных программ (программ-вирусов) и программных закладок;

- применение межсетевого экранирования;
- анализ защищённости информационных систем персональных данных НКО с применением специализированных программных средств (сканеров безопасности);
- резервное копирование информации;
- обеспечение восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;
- учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
- систематическое проведение мониторинга действий пользователей, проведение разбирательств по фактам нарушения требований безопасности персональных данных.

6.4.4. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

6.5. Мероприятия по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации

6.5.1. Обработка персональных данных без использования средств автоматизации осуществляется в режиме коммерческой тайны в соответствии с документом «Положение по обеспечению сохранности коммерческой тайны в НКО «ОРС» (ОАО)».

6.5.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

6.5.3. 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 ПДн, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6.5.4. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

6.5.5. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы:

- о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки.

6.5.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес НКО, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых НКО способов обработки персональных данных;
- при необходимости получения письменного согласия на обработку персональных данных типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.5.7. Подготовка документов, содержащих персональные данные, осуществляется сотрудниками, имеющими допуск к обработке персональных данных.

6.5.8. Печать документов, содержащих персональные данные, производится исполнителями документов.

6.5.9. Входные двери помещений, где хранятся документы, содержащие персональные данные, должны быть оборудованы замками, гарантирующими надежное закрытие помещения во внерабочее время.

Документы, содержащие персональные данные, хранятся в запираемых шкафах.

6.5.10. После окончания рабочего дня сейфы, металлические шкафы и двери помещений, не оборудованные кодовыми замками, запираются.

О фактах утраты ключа от сейфа, металлического шкафа или входной двери помещения, где хранятся документы, содержащие персональные данные, сообщается руководителю структурного подразделения. Замок этого помещения или двери помещения должны быть заменены.

Хранение документов, содержащих персональные данные в сейфах, помещениях, от которых утрачены ключи, до замены замка или изменения его секрета запрещается.

6.5.11. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7. Контроль выполнения требований настоящей Политики

7.1. Контроль выполнения требований настоящей Политики осуществляется путем проведения внутренних проверок уполномоченными лицами в соответствии с внутренним регламентом. В ходе внутренних проверок осуществляются мероприятия, определенные действующим законодательством Российской Федерации в области персональных данных, а так же требования, предъявляемые к системе защиты ПДн информационных систем персональных данных НКО.

8. Ответственность за нарушение требований настоящей Политики

8.1. Нарушение настоящей Политики может повлечь за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

8.2. Сотрудник НКО, который в связи с исполнением трудовых обязанностей получил доступ к персональным данным, в случае умышленного или неосторожного разглашения этой информации, при отсутствии в действиях такого сотрудника состава

преступления, несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации.

8.3. Юридическое лицо, не выполнившее установленные законом обязанности по обеспечению конфиденциальности и безопасности персональных данных, несет ответственность в соответствии с законодательством Российской Федерации.

Приложение 1. Перечень персональных данных, обрабатываемых в НКО «ОРС» (ОАО).

Приложение 2. Перечень информационных систем НКО «ОРС» (ОАО), обрабатывающих персональные данные.

Приложение 3. Перечень актуальных угроз безопасности персональных данных при их обработке в информационных системах НКО «ОРС» (ОАО).

Приложение 4. АКТ определения необходимого уровня защищённости информационных систем персональных данных.