УТВЕРЖДЕНО
приказом директора
АО «НФК-Сбережения»
№ П/240119/1 от 24.01.2019
(с изменениями, внесенными
приказом № П/211119/2 от 21.11.2019,
приказом № П/300421/2 от 30.04.2021)

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЦЕЛЯХ СОБЛЮДЕНИЯ ПРИНЦИПОВ И УСЛОВИЙ ИХ ОБРАБОТКИ, КОНФИДЕНЦИАЛЬНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2021 г.

СОДЕРЖАНИЕ

1. Общие положения

1.1. Настоящее Положение определяет политику в отношении обработки персональных данных, содержит сведения о реализуемых требованиях к защите персональных данных и условия защиты персональных данных физических лиц в целях их обработки Акционерным обществом «Инвестиционная компания «НФК – Сбережения» (далее – Оператор).

1.2. 1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Закон о персональных данных), Трудовым кодексом Российской Федерации, постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами в области защиты персональных данных.

1.3. Обработка персональных данных Оператором осуществляется в целях заключения и исполнения Оператором договоров, в том числе договоров присоединения, включая договоры о предоставлении пользователям доступа к администрируемому оператором электронному сервису, предназначенному для оказания Оператором услуг, состоящих в фиксации информации о волеизъявлении пользователей на заключение гражданско-правовой сделки, в целях исполнения функций работодателя, выполнения требований действующего законодательства, в том числе Федерального закона от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», информационного обеспечения рабочих процессов и для формирования общедоступных внутри информационной системы Оператора источников персональных данных.

1.4. Правовые основания обработки персональных данных:

Правовыми основаниями обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Оператор осуществляет обработку персональных данных, включая, но не ограничиваясь:

Конституция Российской Федерации;

Гражданский кодекс Российской Федерации;

Трудовой кодекс Российской Федерации

Налоговый кодекс Российской Федерации;

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 1 апреля 1996 года № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;

Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти, нормативные акты Центрального Банка Российской Федерации;

Устав Оператора и локальные нормативные акты Оператора;

Согласие субъектов на обработку персональных данных.

1.5. Специальные термины и понятия используются в настоящем положении в значении, установленном действующим законодательством и подзаконными нормативными правовыми актами.

1.6. Копия Положения предоставляется по просьбе заинтересованных лиц без ограничений. Оператор при осуществлении сбора персональных данных с использованием информационнотелекоммуникационных сетей публикует на сайте Оператора **www.nfksber.ru** настоящее Положение.

2. Понятие и состав персональных данных

2.1. Под персональными данными понимается информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, данные документов, удостоверяющих личность, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, и иная информация, которая необходима Оператору в связи с реализацией трудовых отношений между работодателем и работником, и/или в целях заключения и исполнения Оператором договоров, в том числе договоров об оказании услуг Оператором, и/или в целях выполнения требований действующего законодательства, в том числе Федерального закона от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации», Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

2.2. На лиц, которые предоставили Оператору персональные данные в целях реализации договорных отношений, но договор с ними заключен не был, или прекратили договорные отношения с Оператором, данное Положение распространяется в части, не противоречащей положениям законодательства Российской Федерации.

3. Принципы и условия обработки персональных данных

3.1. Персональные данные обрабатываются на основе принципов:

а) законности целей и способов обработки персональных данных и добросовестности;

б) обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам Оператора в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

в) соответствия объема и характера обрабатываемых персональных данных, способов их обработки целям обработки персональных данных. Оператор не имеет права получать и обрабатывать персональные данные Субъекта персональных данных о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ Оператор вправе получать и обрабатывать данные о частной жизни Субъекта персональных данных только с его письменного согласия. Оператор не имеет права получать и обрабатывать персональные данные Субъекта персональных данных о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ;

г) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к заявленным при их сборе целям. Все персональные данные Субъекта персональных данных следует получать у него самого. В случаях, предусмотренных Законом о персональных данных, Оператор должен сообщить Субъекту персональных данных о целях и способах обработки персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта персональных данных дать письменное согласие на их получение (в случае, если такое согласие требуется);

д) недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

е) защиты персональных данных Субъекта персональных данных от неправомерного доступа и их использования или утраты. Оператор должен обеспечить такую защиту за счет собственных средств и в порядке, установленном законодательством РФ.

3.2. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных действующим законодательством. Обработка персональных данных допускается в следующих случаях:

а) обработка персональных данных осуществляется с согласия Субъекта персональных данных на обработку его персональных данных;

б) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей;

в) 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 (далее - исполнение судебного акта);

г) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

д) 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;

е) обработка персональных данных необходима для защиты жизни и здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

ж) обработка персональных данных необходима для осуществления прав и законных интересов Оператора или третьих лиц, в том числе, в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы Субъекта персональных данных;

з) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

и) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Закона о персональных данных, при условии обязательного обезличивания персональных данных;

к) 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);

л) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;

м) в других случаях, предусмотренных действующим законодательством.

3.3. Оператор вправе поручить обработку персональных данных другому лицу с согласия Субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении Оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Закона о персональных данных.

3.3. Лицо, осуществляющее обработку персональных данных по поручению Оператора, не обязано получать согласие Субъекта персональных данных на обработку его персональных данных.

3.4. В случае, если Оператор поручает обработку персональных данных другому лицу, ответственность перед Субъектом персональных данных за действия указанного лица несет Оператор. Лицо, осуществляющее обработку персональных данных по поручению Оператора, несет ответственность перед Оператором.

3.5. Оператор и уполномоченные им лица, ответственные за организацию обработки персональных данных, лица, осуществляющие обработку персональных данных / имеющие доступ к персональным данным, должны быть ознакомлены под роспись с документами, устанавливающими порядок обработки персональных данных.

3.6. Персональные данные должны храниться в форме, позволяющей определить Субъекта персональных данных, но не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

4. Порядок обработки персональных данных

4.1. Обработка персональных данных Субъектов персональных данных осуществляется с их письменного согласия, если иное не предусмотрено действующим законодательством.

4.2. В целях обеспечения защиты персональных данных Субъекты персональных данных вправе:

а) получать полную информацию о своих персональных данных и способе обработки этих данных;

б) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, за исключением случаев, предусмотренных Федеральным законом «О персональных данных»;

в) требовать внесения необходимых изменений, уничтожения или блокирования соответствующих персональных данных, которые являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

г) обжаловать в порядке, установленном законодательством Российской Федерации, действия (бездействие) уполномоченных должностных лиц.

4.3. Обработка персональных данных Субъектов персональных данных может осуществляться как с использованием средств автоматизации, так и без использования таких средств.

Оператор обрабатывает персональные данные следующих категорий субъектов персональных данных:

персональные данные соискателей (лиц, претендующих на трудоустройство к Оператору);

персональные данные работников Оператора;

персональные данные лиц, занимающих должности в органах управления Оператора, включая работников Оператора, но не ограничиваясь названным;

персональные данные физических лиц, включенных в список инсайдеров Оператора, а также лиц, связанных с лицами, указанными в пунктах 7 и 13 статьи 4 Федерального закона от 27 июля 2010 года № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;

персональные данные физических лиц, являющихся аффилированными лицами Оператора;

персональные данные клиентов и контрагентов Оператора, представителей клиентов и/или контрагентов Оператора;

персональные данные пользователей администрируемых Оператором электронных сервисов.

4.4. Обработка персональных данных осуществляется путем:

1) получения оригиналов необходимых документов, предоставляемых субъектами персональных данных;

2) получения заверенных в установленном порядке копий документов, содержащих персональные данные, или копирования оригиналов документов;

3) формирования персональных данных в ходе кадровой работы;

4) получения информации, содержащей персональные данные, в устной и письменной форме непосредственно от Субъектов персональных данных;

5) получения персональных данных в ответ на запросы, направляемые Оператором в органы государственной власти, государственные внебюджетные фонды, иные государственные органы, органы местного самоуправления, коммерческие и некоммерческие организации, физическим лицам в случаях и порядке, предусмотренных законодательством Российской Федерации;

6) получения персональных данных из общедоступных источников;

7) получения персональных данных из государственных информационных систем;

8) фиксации (регистрации) персональных данных в журналах, книгах, реестрах и других учетных формах;

9) внесения персональных данных в информационные системы Оператора;

10) использования иных средств и способов фиксации персональных данных, получаемых в рамках осуществляемой Оператором деятельности.

При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обеспечивает запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6 Закона Федерального закона «О персональных данных».

4.5. Все необходимые персональные данные следует получать лично у Субъекта персональных данных или у его надлежащим образом уполномоченного представителя, за исключением случаев, когда в соответствии с федеральным законом персональные данные Субъекта персональных данных могут быть предоставлены третьим лицом, или включены в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты государства и общественного порядка.

Персональные данные могут быть получены Оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Закона о персональных данных. Если персональные данные получены не от Субъекта персональных данных, Организация, если иное не предусмотрено действующим законодательством, должна сообщить предоставить Субъекту персональных данных следующую информацию:

наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

права Субъекта персональных данных;

источник получения персональных данных.

4.6. Хранение персональных данных осуществляется соответственно целям обработки персональных данных. Лица, ответственные за обработку персональных данных, несут обязанности по обеспечению конфиденциальности персональных данных (за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных) и сохранности документов и иных носителей, содержащих персональные данные, от несанкционированного доступа посторонних лиц, уничтожения и копирования.

4.7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, 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. Документы, содержащие персональные данные, подлежат уничтожению по достижении целей их обработки и/или в случае утраты необходимости в их достижении, по окончании сроков хранения соответствующих документов, предусмотренных законодательством, если иное не установлено законодательством Российской Федерации.

4.8. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

– уменьшение перечня обрабатываемых сведений;
– замена части сведений идентификаторами;
– обобщение – понижение точности некоторых сведений;
– понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);
– другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

Для обезличивания персональных данных могут быть использованы любые способы, явно не запрещенные законодательством.

4.9. В целях организации обработки персональных данных Оператор назначает специальное ответственное лицо (далее - «Лицо, ответственное за организацию обработки персональных данных»).

5. Особенности обработки персональных данных Субъектов персональных данных, осуществляемой без использования средств автоматизации

5.1. При обработке персональных данных без использования средств автоматизации не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

5.2. Уничтожение или обезличивание персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

5.3. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем внесения изменений в текст, содержащий персональные данные, если это допустимо с учетом общепринятой практики работы с соответствующим материальным носителем, или путем изготовления нового материального носителя с уточненными персональными данными.

5.4. В целях обеспечения безопасности персональных данных при обработке, осуществляемой без использования средств автоматизации, Оператор принимает следующие меры:

- исключение несанкционированного доступа к персональным данным (материальным носителям);
- обеспечение сохранности персональных данных (материальных носителей).

6. Особенности обработки персональных данных Субъектов персональных данных в информационных системах

6.1. Обработка персональных данных Оператором может осуществляться в информационных системах, в том числе, но не ограничиваясь названным, в информационных системах, предназначенных для ведения бухгалтерского учета и/или кадровой работы и/или внутреннего учета, в том числе учета валютных и иных операций, и/или депозитарного учета, а также в информационных системах, предназначенных для администрирования электронных сервисов Оператора.

6.2. Безопасность персональных данных, обрабатываемых в информационных системах, достигается путем соблюдения Оператором следующих требований:

- 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;
- обеспечение сохранности носителей персональных данных.

6.3. Оператор принимает следующие меры по обеспечению безопасности персональных данных при их обработке в информационных системах:

6.3.1. Идентификация и аутентификация субъектов доступа и объектов доступа:

- идентификация и аутентификация пользователей информационных систем;
- управление идентификаторами, в том числе, создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

6.3.2. Управление доступом субъектов доступа к объектам доступа:

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе, внешних пользователей;
- реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

6.3.3. Антивирусная защита:

- реализация антивирусной защиты;
- обновление базы данных признаков вредоносных компьютеров программ (вирусов).

6.3.4. Контроль (анализ) защищенности персональных данных:

- контроль установки обновление программного обеспечения, включая обновление программного обеспечения средств защиты информации.

6.3.5. Защита технических средств:

- контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;.

6.3.6. Защита информационной системы, ее средств, систем связи и передачи данных:

- обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

7. Меры по обеспечению сохранности персональных данных и исключению несанкционированного доступа к персональным данным

7.1. Обеспечение безопасности персональных данных при их обработке Оператором осуществляется в соответствии с законодательством Российской Федерации и требованиями уполномоченного органа государственной власти по защите прав субъектов персональных данных, федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности, и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

7.2. Оператор предпринимает необходимые организационные и технические меры для защиты персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

7.3. Меры защиты, реализуемые Оператором при обработке персональных данных, включают:

- принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
- назначение должностных лиц, ответственных за обеспечение безопасности персональных данных в подразделениях и информационных системах Оператора;
- организацию и проведение методической работы с работниками, осуществляющими обработку персональных данных;
- создание необходимых условий для работы с материальными носителями и информационными системами, в которых обрабатываются персональные данные;
- организацию учета материальных носителей персональных данных и информационных систем, в которых обрабатываются персональные данные;
- хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним;
- обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации;
- обеспечение раздельного хранения материальных носителей персональных данных, на которых содержатся персональные данные разных категорий или содержатся персональные данные, обработка которых осуществляется в разных целях;
- осуществление внутреннего контроля за соблюдением Оператором законодательства Российской Федерации и локальных нормативных актов Оператора при обработке персональных данных.

7.4. Ответственность за нарушение требований законодательства Российской Федерации и нормативных актов Оператора в сфере обработки и защиты персональных данных определяется в соответствии с законодательством Российской Федерации.

8. Работа с обезличенными персональными данными

8.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

8.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

8.2.1. Уменьшение перечня обрабатываемых сведений;

8.2.2. Замена части сведений идентификаторами;

8.2.3. Обобщение – понижение точности некоторых сведений;

8.2.4. Понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

8.2.5. Другие способы.

8.3. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

8.4. Для обезличивания персональных данных могут быть использованы любые способы, явно не запрещенные законодательством.

8.5. Перечень должностей работников Оператора, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в Приложении № 3 к настоящему Положению. Решение о необходимости обезличивания персональных данных принимает руководитель Оператора, с указанием способа обезличивания персональных данных.

8.6. Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

8.7. Обработка обезличенных персональных данных осуществляется с соблюдением требований, установленных настоящим Положением к обработке необезличенных персональных данных.

9. Порядок внутреннего контроля за соблюдением требований по обработке и обеспечению безопасности данных

9.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в организации проводятся периодические проверки условий обработки персональных данных. Проверки осуществляются лицом, ответственным за организацию обработки персональных данных, не реже одного раза в год.

9.2. При осуществлении внутреннего контроля за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, производится проверка:

- соблюдения принципов обработки персональных данных;
- соответствия локальных актов Оператора в области персональных данных действующему законодательству Российской Федерации;
- выполнения сотрудниками Оператора требований и правил (в том числе особых) обработки персональных данных;
- перечней персональных данных, используемых для решения задач и функций структурными подразделениями Оператора и необходимости обработки персональных данных;
- правильности осуществления сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных;
- актуальности перечня должностей сотрудников Оператора, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- актуальности перечня должностей сотрудников Оператора, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- соблюдения прав Субъектов персональных данных, чьи персональные данные обрабатываются Оператором;
- соблюдения обязанностей Оператора, предусмотренных действующим законодательством в области персональных данных;
- порядка взаимодействия с Субъектами персональных данных, чьи персональные данные обрабатываются Оператором, в том числе соблюдения сроков предусмотренных действующим законодательством в области персональных данных, соблюдения требований по уведомлениям, порядка разъяснения Субъектам персональных данных необходимой информации, порядка реагирования на обращения Субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий Субъектами персональных данных;
- наличия необходимых согласий Субъектов персональных данных, чьи персональные данные обрабатываются Оператором;
- знания и соблюдения сотрудниками Оператора положений действующего законодательства Российской Федерации в области персональных данных;
- знания и соблюдения сотрудниками Оператора положений локальных актов Оператора в области обработки и обеспечения безопасности персональных данных;
- знания и соблюдения сотрудниками Оператора инструкций, руководств и иные эксплуатационных документов на применяемые средства автоматизации, в том числе программное обеспечение, и средства защиты информации;
- соблюдения сотрудниками Оператора конфиденциальности персональных данных;

- иных вопросов, связанных с обработкой персональных данных Оператором.

9.3. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Оператора докладывает лицо, ответственное за организацию обработки персональных данных Оператором.

9.4. Во всем остальном, что не предусмотрено условиями настоящего Положения, применяются нормы действующего законодательства, подзаконных нормативных правовых актов и локальных нормативных правовых актов (внутренних документов) Оператора.

10. Ответы на запросы субъектов на доступ к персональным данным. Актуализация, исправление, удаление и уничтожение персональных данных

10.1. Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя.

Сведения предоставляются в доступной форме, в них не включаются персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Если в обращении (запросе) субъекта персональных данных не отражены в соответствии с требованиями Федерального закона «О персональных данных» все необходимые сведения или субъект не обладает правами доступа к запрашиваемой информации, то ему направляется мотивированный отказ.

Запрос должен содержать данные основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись (в том числе электронная) субъекта персональных данных или его представителя.

Сведения, указанные в части 7 статьи 14 Федерального закона «О персональных данных», предоставляются субъекту персональных данных или его представителю Оператором при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с частью 8 статьи 14 Федерального закона «О персональных данных» в том числе, если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

10.2. В срок, не превышающий 30 дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Оператор вносит в них необходимые изменения.

В срок, не превышающий 30 дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Оператор уничтожает такие персональные данные.

Оператор уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

10.3. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Оператор прекращает их обработку или обеспечивает прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Оператором и субъектом персональных данных либо если Оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

В случае отсутствия возможности уничтожения персональных данных в течение вышеуказанного срока Оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

В случае отзыва субъектом персональных данных согласия на обработку персональных данных Оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в части 2 статьи 9 Федерального закона «О персональных данных».

11. Заключительные положения

11.1. Настоящее Положение является общедоступным документом Оператора.

11.2. Настоящее Положение подлежит изменению в случае принятия нормативных актов, устанавливающих новые требования по обработке и защите персональных данных или внесения изменений в действующие нормативные правовые акты.

11.3. В целях реализации политики в области персональных данных, определенной настоящим Положением, Оператор вправе принимать и утверждать иные локальные нормативные акты в порядке, установленном действующим законодательством и внутренними документами Оператора.

Приложение № 1. Объем и категории персональных данных, обрабатываемых Оператором и подлежащих защите, категории субъектов персональных данных

В зависимости от целей обработки, Оператором могут обрабатываться персональные данные следующих категорий субъектов:

1. Соискатели на должности:
- фамилия, имя, отчество;
- пол;
- год, месяц, день и место рождения;
- фотография;
- адрес места регистрации / места жительства;
- гражданство;
- образование, квалификация (год окончания учебного заведения), профессиональная подготовка, сведения о повышении квалификации;
- сведения о трудовой деятельности, в том числе, наличие поощрений, награждений или дисциплинарных взысканий;
- профессия;
- контактная информация.

2. Работники Оператора:
- фамилия, имя, отчество;
- пол;
- год, месяц, день и место рождения;
- фотография;
- адрес места регистрации / места жительства;
- гражданство;
- сведения из личных карточек работников;
- образование, квалификация (номера, серии дипломов, год окончания учебного заведения), профессиональная подготовка, сведения о повышении квалификации;
- сведения о трудовой деятельности, в том числе, наличие поощрений, награждений или дисциплинарных взысканий;
- профессия;
- табельный номер;
- идентификационный номер налогоплательщика;
- страховой номер индивидуального лицевого счета (СНИЛС);
- семейное положение, состав семьи (степень родства, Ф. И. О, год рождения);
- сведения об удержании алиментов;
- сведения о доходе с предыдущего места работы
- паспортные данные;
- сведения о воинском учете;
- сведения о нетрудоспособности, временной нетрудоспособности, инвалидности
- банковские реквизиты;
- контактная информация;
- иные персональные данные, представляемые в соответствии с требованиями трудового законодательства.

3. Лица, занимающие должности в органах управления Оператора:
- фамилия, имя, отчество;
- гражданство;
- место жительства;
- реквизиты документа, удостоверяющего личность;
- ИНН.

4. Клиенты и (или) представители клиентов:
- фамилия, имя, отчество;
- год, месяц, день и место рождения;
- адрес места регистрации / места жительства;
- паспортные данные;
- идентификационный номер налогоплательщика;
- банковские реквизиты;
- контактная информация;
- иные персональные данные, предоставляемые в соответствии с требованиями законодательства, предъявляемыми к Оператору как профессиональному участнику рынка ценных бумаг.

5. Физические лица, включенные в список инсайдеров Оператора, а также лица, связанные с лицами, указанными в пунктах 7 и 13 статьи 4 Федерального закона от 27 июля 2010 года № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»:
- фамилия, имя, отчество;
- год, месяц, день и место рождения;
- адрес места регистрации / места жительства;
- паспортные данные.

6. Физические лица, являющиеся аффилированными лицами Оператора:
- фамилия, имя, отчество;
- гражданство;
- место жительства;
- реквизиты документа, удостоверяющего личность;
- ИНН.

7. Иные контрагенты Оператора:
- фамилия, имя, отчество;
- год, месяц, день и место рождения;
- адрес места регистрации / места жительства;
- паспортные данные;
- идентификационный номер налогоплательщика;
- номер свидетельства государственного пенсионного страхования;
- банковские реквизиты;
- контактная информация;
- иные персональные данные, предоставляемые в соответствии с требованиями действующего законодательства.

8. Пользователи администрируемых Оператором электронных сервисов/представители пользователей:
- фамилия, имя, отчество (при наличии);
- дата рождения;
- реквизиты документа, удостоверяющего личность;
- идентификационный номер налогоплательщика;
- номер свидетельства государственного пенсионного страхования;
- банковские реквизиты;
- номера телефонов;
- адреса электронной почты;
- адреса проживания.

Приложение № 2. Перечень должностей лиц, имеющих доступ к персональным данным и осуществляющих обработку персональных данных

ПЕРЕЧЕНЬ
должностей лиц, имеющих доступ к персональным данным и осуществляющих обработку персональных данных

1. ______________________________ - в отношении персональных данных, обрабатываемых в связи с реализацией трудовых отношений.
2. ______________________________ - в отношении персональных данных, обрабатываемых в связи с оказанием Оператором услуг.
3. ______________________________ - в отношении персональных данных, обрабатываемых в связи с заключением и исполнением Оператором договоров (за исключением договоров об оказании Оператором услуг)

Приложение № 3. Перечень должностей лиц, ответственных за обезличивание персональных данных

ПЕРЕЧЕНЬ
должностей лиц, ответственных за обезличивание персональных данных

1. ______________________________ - в отношении персональных данных, обрабатываемых в связи с реализацией трудовых отношений.
2. ______________________________ - в отношении персональных данных, обрабатываемых в связи с оказанием Оператором услуг.
3. ______________________________ - в отношении персональных данных, обрабатываемых в связи с заключением и исполнением Оператором договоров (за исключением договоров об оказании Оператором услуг)

Приложение № 4. Перечень мест хранения персональных данных

ПЕРЕЧЕНЬ
мест хранения персональных данных

№ п/п	Носитель	Места хранения	Ответственное лицо	Примечание
1	Жесткие диски серверов и системы хранения данных	В рабочем режиме – серверы В режиме ремонта – обслуживающая организация		---
2	Переносные носители	У пользователя информационной системы персональных данных	Пользователь информационной системы персональных данных	Хранение должно производиться в охраняемых помещениях
3	Бумажные носители	____________________________________ - в отношении персональных данных, обрабатываемых в связи с реализацией трудовых отношений. ____________________________________ - в отношении персональных данных, обрабатываемых в связи с оказанием Оператором услуг. ____________________________________ - в отношении персональных данных, обрабатываемых в связи с заключением и исполнением Оператором договоров (за исключением договоров об оказании Оператором услуг)		Хранение должно производиться в охраняемых помещениях

Приложение № 5. Журнал учета обращений субъектов персональных данных и ответов на них

ЖУРНАЛ УЧЕТА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОТВЕТОВ НА НИХ

№ п/п	Запрашивающее лицо (ФИО, должность) / законный представитель / орган по защите прав Субъектов персональных данных	Реквизиты запроса (вх. №, дата запроса)	Краткое содержание запроса	Результат рассмотрения запроса	Реквизиты ответа (исх. №, дата ответа)	Подпись лица, ответственного за предоставление информации

Приложение № 6. Акт об уничтожении персональных данных, обрабатываемых АО «НФК – Сбережения»

А К Т № ______
об уничтожении персональных данных, обрабатываемых
АО «НФК – Сбережения»

Комиссия в составе:
Председатель комиссии ______________________ ______________________
(ФИО) *(должность)*

Члены комиссии:
______________________ ______________________
______________________ ______________________
______________________ ______________________
провела анализ персональных данных, хранящихся на носителях и/или в информационных системах *(нужное подчеркнуть)*, и установила, что информация, записанная на них в процессе их эксплуатации, подлежит уничтожению:

№ п/п	**Сведения, характеризующие подлежащую уничтожению информацию**	**Тип носителя, сведения, характеризующие носитель подлежащей уничтожению информации**	**Кол-во уничтожен-ных носителей**	**Метод уничтожения (удаление файла, записи базы данных, носителя информации и т.п.)**	**Отметка об уничтожении и проверке результатов уничтожения**	**Дата**	**Примечания**

Всего уничтожено носителей ____
(цифрами и прописью)

Председатель комиссии ______________________ ______________________

Члены комиссии:
______________________ ______________________
______________________ ______________________
______________________ ______________________

Приложение № 7. Журнал проведения инструктажа по соблюдению правил обработки персональных данных и допуска сотрудников к работе с персональными данными в АО «НФК-Сбережения»

ЖУРНАЛ ПРОВЕДЕНИЯ ИНСТРУКТАЖА ПО СОБЛЮДЕНИЮ ПРАВИЛ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ДОПУСКА СОТРУДНИКОВ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ В АО «НФК – СБЕРЕЖЕНИЯ»

№ п/п	Должность, ФИО инструктируемого	Дата проведения инструктажа	Цель инструктажа, доводимые инструкции	Отметка о прохождении инструктажа (ФИО и подпись инструктируемого)	ФИО и подпись инструктирующего

Приложение № 8. Лист ознакомления работников с Положением об обработке персональных данных АО «НФК – Сбережения»

ЛИСТ ОЗНАКОМЛЕНИЯ РАБОТНИКОВ

с Положением об обработке персональных данных АО «НФК – Сбережения»

Должность	ФИО	Подпись	Дата ознакомления

Приложение № 9. Отчет о проведенной проверке при осуществлении внутреннего контроля за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных

ОТЧЕТ
о проведенной проверке при осуществлении внутреннего контроля за соблюдением Оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных

1. Основания и цель проведения проверки ______________________.
2. В ходе проведения проверки подтверждены (обнаружены) следующие нарушения законодательства Российской Федерации в сфере персональных данных, иных нормативных правовых актов в области защиты персональных данных и внутренних документов Оператора:

1) Содержание нарушения:_______________.

2) Виновные в них лица: ____________________.

3) Сведения о действиях, совершенных с целью устранения выявленных нарушений (при их наличии): ____

4) Сведения об обращениях Субъектов персональных данных (в случае, если эти обращения связаны с нарушением прав указанных Субъектов или содержат в себе жалобу на действия должностных лиц Оператора): __________________.

3. Другая информация.

Лицо, ответственное за организацию обработки персональных данных ____________________ _________________.

(подпись) *(Ф.И.О.)*

«___» ____________ 20_ г.

Отчет получен: «......» _____________ 20_ г.

Директор ____________________ _________________.

(подпись) *(Ф.И.О.)*