БАНК ОРАНЖЕВЫЙ
Общество с ограниченной ответственностью

УТВЕРЖДЕНО

Решением Правления

ООО Банк Оранжевый

Протокол № 17/10/2014

от 17.10.2014

Положение о порядке обработки персональных данных в ООО Банк Оранжевый

Разработчик: Отдел информационной безопасности
Место хранения: Управление документационного обеспечения
Ограничение доступа: Открытый доступ

Санкт-Петербург
2014

СОДЕРЖАНИЕ

ЛИСТ СОГЛАСОВАНИЯ

Положение о порядке обработки персональных данных в ООО Банк Оранжевый

Проект предоставлен на согласование: 15 октября 2014 года

Должность	**Ф.И.О.**	**Подпись и дата согласования**
Директор по правовому обеспечению	Р.Р. Абрамов	
Начальник Управления риск-менеджмента	О.Ф. Рыськина	
Начальник Управления организационно-технологического развития	И.А. Мошкова	
Руководитель Службы внутреннего аудита	Ю.В. Дворецкая	

1. Термины, определения, сокращения.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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

Доступ к персональным данным - возможность получения персональных данных и их использования.

Защита от НСД - предотвращение или существенное затруднение НСД.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Конфиденциальность персональных данных - обязательное для соблюдения Банком или иным получившим доступ к персональным данным лицом требование не раскрывать третьим лицам и не допускать распространение персональных данных без согласия субъекта персональных данных или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия, НСД) - доступ к персональным данным или действия с персональными данными, нарушающие установленные права и (или) правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

ОИБ – Отдел информационной безопасности;

ООО Банк Оранжевый (Банк) - юридическое лицо, организующее и осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

ОСАиТ – отдел системного администрирования и телекоммуникаций;

Персональные данные (ПДн) - 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.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Санкционированный доступ – доступ к персональным данным, не нарушающий правила разграничения доступа.

Система защиты персональных данных (СЗПДн) - организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и

информационных технологий, используемых в информационных системах.
Субъект доступа – лицо или процесс, действие которого регламентируется правилами разграничения доступа.
Субъект ПДн - физическое или юридическое лицо, выступающее в качестве стороны сделки, целью которой является совершение банковской операции, банковской сделки или операции, совершаемой в процессе хозяйственной деятельности, с участием Банка.
Технические средства - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в ИСПДн.
Угроза безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
УДО – Управление документационного обспечения;
УИТ – Управление информационных технологий;
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. Общие положения

2.1. Положение о порядке обработки персональных данных в ООО Банк Оранжевый (далее – Положение) разработано в соответствии с требованиями законодательства Российской Федерации, регламентирующего вопросы защиты персональных данных, и требований (рекомендаций) Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - Роскомнадзор), Федеральной службы безопасности Российской Федерации (далее - ФСБ), Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России), Центрального банка Российской Федерации (Банка России) (далее - Регуляторы, если по смыслу не требуется детализация).
2.2. Целями Положения являются:

- обеспечение требований по защите прав и свобод человека и гражданина при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- исключение несанкционированных действий при обработке персональных данных, хранящихся в Банке;
- обеспечение конфиденциальности сведений, составляющих персональные данные, и предотвращение возможного совершения противоправных деяний в отношении субъектов ПДн;
- исключение возможного противоправного разглашения персональных данных третьим лицам вне зависимости от того может ли такое разглашение нанести ущерб Банку или субъектам ПДн.

2.3. Основной задачей настоящего Положения является определение требований по работе со всеми видами носителей информации, содержащих персональные данные, и определение содержания и порядка осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах Банка.

2.4. Положение основывается на следующих принципах:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Банка;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- хранение ПДн, цели обработки которых заведомо несовместимы, на отдельных съемных носителях, в отдельных базах данных ИСПДн.;
- уничтожения персональных данных после достижения целей их обработки, а также если ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- личной ответственности работников Банка за сохранность и конфиденциальность персональных данных, а также носителей информации, содержащих персональные данные;
- наличия процедур доступа работников Банка к ИСПДн и документам, содержащим ПДн.

2.5. Положение является обязательным для исполнения всеми работниками ООО Банк Оранжевый, имеющими доступ к персональным данным, предоставляемый на основании положений трудового договора и должностных инструкций.

2.6. Банком осуществляется охрана помещений, в которых ведется обработка персональных данных, что позволяет обеспечивать сохранность ИСПДн, носителей персональных данных и средств защиты ИСПДн, а также исключает возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.7. При вступлении в силу законодательных и нормативных актов Российской Федерации, предусматривающих иные требования по обеспечению защиты персональных данных, в данное Положение будут вноситься необходимые дополнения и изменения. До приведения настоящего Положения в соответствие с новыми законодательными и нормативными актами Российской Федерации оно применяется в части, не противоречащей указанным актам.

3. Порядок обработки персональных данных.

3.1. При обработке персональных данных в ИСПДн Банка должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного разглашения персональных данных лицам, не имеющим права доступа к такой информации;
- проведение мероприятий, направленных на предотвращение НСД к персональным данным по техническим каналам;
- своевременное обнаружение фактов несанкционированного разглашения и НСД;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено функционирование данных средств;
- возможность незамедлительного восстановления персональных данных,

модифицированных или уничтоженных вследствие несанкционированного доступа к ним либо в результате иных причин;
- обезличивание персональных данных в случаях, когда технические возможности ИСПДн позволяют это осуществить, и признана целесообразность проведения обезличивания;
- постоянный контроль обеспечения надлежащего уровня защищенности персональных данных.

3.2. При обработке персональных данных ОИБ вырабатывает необходимые организационные и технические меры для защиты персональных данных от неправомерной обработки, которые утверждаются Правлением Банка и реализуются силами ОИБ и УИТ или с привлечением сторонних организаций, а также соблюдает следующие требования:

3.2.1. Хранение и защита персональных данных от неправомерного их использования или утраты обеспечивается Банком за счет собственных средств в порядке, установленном законодательством Российской Федерации.

3.2.2. Если предоставление персональных данных является обязательным для субъекта ПДн в соответствии с федеральным законом, работник Банка, осуществляющий сбор ПДн, обязан разъяснить субъекту ПДн юридические последствия отказа предоставить его персональные данные.

3.2.3. Если персональные данные получены не от субъекта персональных данных, руководитель подразделения, получившего ПДн, за исключением случаев, перечисленных в пункте 3.2.4 настоящего положения, до начала обработки таких персональных данных предоставляет субъекту персональных данных следующую информацию:
- наименование и адрес Банка;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- права субъекта персональных данных;
- источник получения персональных данных.

Предоставление сведений осуществляется путем направления Уведомления о наличии обработки персональных данных (по форме Приложения 4 к настоящему Положению).

3.2.4. Банк освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 3.2.3 настоящего положения, в случаях, если:
- субъект персональных данных уведомлен об осуществлении обработки его персональных данных Банком;
- персональные данные получены Банком на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
- персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
- предоставление субъекту персональных данных сведений, предусмотренных пунктом 3.2.3 настоящего положения, нарушает права и законные интересы третьих лиц.

3.2.5. Персональные данные относятся к конфиденциальной информации ограниченного доступа и могут быть использованы для целей оказания услуг Банком, защиты интересов Банка, субъектов ПДн с обязательным исполнением требований защиты прав и свобод человека и гражданина, неприкосновенности частной жизни, личной и семейной тайны.

3.2.6. Обеспечение конфиденциальности персональных данных не требуется в случае их обезличивания, а также в отношении общедоступных персональных данных.

3.2.7. Банк не собирает и не обрабатывает персональные данные о расовой, национальной

принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, частной жизни субъектов ПДн, за исключением случаев, предусмотренных действующим законодательством Российской Федерации.

3.2.8. При поступлении обращения субъекта ПДн, его законного представителя или уполномоченного органа по защите прав субъектов персональных данных, оно регистрируется УДО в Журнале учета обращений субъектов персональных данных (законных представителей субъектов персональных данных) (Приложение 11 к настоящему Положению) и передается руководителю подразделения, обрабатывающего ПДн субъекта. Руководитель подразделения готовит ответ и согласовывает его с Отделом юридического консалтинга и ОИБ. Ответ подписывается:

- в Головном Офисе - Председателем Правления или лицом его замещающим,
- в Дополнительных и Операционных офисах – Управляющим,
- в Филиалах – Директором филиала.

После подписания в ГО ответ передается в УДО, где он регистрируется и направляется субъекту ПДн. В Филиале ответ регистрируется и направляется субъекту ПДн (законному представителю субъекта ПДн) лицом, ответственным за делопроизводство

Ведение Журнала учета обращений субъектов ПДн (законных представителей субъектов ПДн) допускается в электронном виде.

3.2.9. В случае выявления недостоверных персональных данных или неправомерной обработки персональных данных при обращении или по запросу субъекта ПДн или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных, Комиссией, состоящей из Руководителя подразделения, обрабатывающего ПДн субъекта и работника ОИБ, проводится проверка достоверности и правомерности обработки ПДн.

3.2.10. В случае подтверждения факта недостоверности персональных данных Руководитель подразделения, в которое поступило обращение, на основании документов, представленных субъектом ПДн или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, уточняет персональные данные в течение 7 (семи) рабочих дней со дня получения Банком таких сведений, и снять их блокирование.

3.2.11. После уточнения персональных данных Руководитель подразделения уведомляет об этом субъекта ПДн или его законного представителя, а в случае поступления запроса от уполномоченного органа по защите прав субъектов персональных данных, также информирует указанный орган путем направления Уведомления о внесении изменений в некорректные персональные данные (по форме Приложения 5 к настоящему Положению).

3.2.12. В случае передачи недостоверных персональных данных третьим лицам Руководитель подразделения, передавшего сведения, уведомляет об этом указанных лиц путем направления Письма о внесении изменений в переданные персональные данные (по форме Приложения 6 к настоящему Положению).

3.2.13. В случае подтверждения факта неправомерной обработки персональных данных Руководитель подразделения, обнаружившего данный факт, прекращает неправомерную обработку персональных данных в срок, не превышающий 3 (трех) рабочих дней с момента выявления. В случае если обеспечить правомерность обработки персональных данных невозможно, Комиссия по уничтожению ПДн в срок, не превышающий 10 (десяти) рабочих дней с момента выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

3.2.14. О проведенных мероприятиях по устранению допущенных нарушений или уничтожению персональных данных Руководитель подразделения, обрабатывающего ПДн, уведомляет субъекта ПДн или его законного представителя, а в случае поступления запроса

от уполномоченного органа по защите прав субъектов персональных данных, также уведомляет указанный орган путем направления Уведомления о проведенных мероприятиях по факту обнаружения неправомерной обработки персональных данных (по форме Приложения 7 к настоящему Положению).
3.2.15. В случае невозможности обеспечения правомерности обработки персональных данных, ранее переданных Банком третьим лицам, Руководитель подразделения, передавшего ПДН, уведомляет об этом указанных лиц путем направления Письма об удалении персональных данных (по форме Приложения 8 к настоящему Положению).
3.2.16. В случае достижения целей обработки персональных данных Банк обязан прекратить обработку и уничтожить персональные данные в срок, не превышающий 30 (тридцати) дней с момента достижения целей обработки персональных данных, за исключением случаев, когда Банк имеет право осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.
3.2.17. С целью уничтожения персональных данных Банком создается Комиссия из числа работников Банка, выявляющая перечень субъектов персональных данных, информация о которых подлежит уничтожению, ИСПДн, в которых производится обработка указанной информации, а также носители персональных данных, подлежащие уничтожению.
3.2.18. В случае выявления ИСПДн, содержащих сведения о субъектах персональных данных, информация о которых подлежит уничтожению, производится удаление указанных сведений из соответствующих ИСПДн. Результаты удаления фиксируются в Акте удаления персональных данных (по форме Приложения 9 к настоящему Положению).
3.2.19. В случае выявления носителей персональных данных, содержащих сведения о субъектах персональных данных, информация о которых подлежит уничтожению, при возможности и целесообразности производится уничтожение информации на носителях персональных данных с помощью программного обеспечения гарантированного уничтожения информации, в противном случае производится уничтожение указанных носителей персональных данных. Результаты уничтожения фиксируются в Акте уничтожения носителей персональных данных (по форме Приложения 10 к настоящему Положению).
3.2.20. В случае поступления в Банк запроса субъекта ПДн, его законного представителя, уполномоченного органа по защите прав субъектов персональных данных, удовлетворяющего требованиям Федерального закона «О персональных данных», Руководитель подразделения, в которое поступило обращение, сообщает о наличии либо отсутствии обработки Банком персональных данных, относящихся к соответствующему субъекту ПДн путем направления Ответа о наличии обработки персональных данных (по форме Приложения 1 к настоящему Положению) либо Ответа об отсутствии обработки персональных данных (по форме Приложения 2 к настоящему Положению) соответственно. В случае осуществления Банком обработки персональных данных, Банк также предоставляет возможность ознакомления с ними при обращении субъекта ПДн или его законного представителя в течение 30 (тридцати) рабочих дней с момента получения Банком запроса субъекта ПДн или его законного представителя (в соответствии с процедурой, описанной в п. 3.2.8). В случае отказа в предоставлении информации Руководитель подразделения сообщает об этом субъекту ПДн либо его законному представителю путем направления мотивированного Ответа об отказе в предоставлении информации о наличии обработки персональных данных (по форме Приложения 3 к настоящему Положению), содержащего ссылку на положение части 8 статьи 14 Федерального закона «О персональных данных», в срок, не превышающий 30 (тридцати) дней со дня поступления в Банк запроса субъекта ПДн

либо его законного представителя, удовлетворяющего требованиям Федерального закона «О персональных данных».

3.3. При обработке Банком персональных данных субъект ПДн имеет право:

- ознакомиться со своими персональными данными, обрабатываемыми Банком;
- получить информацию о способах, правовых основаниях и целях обработки персональных данных, о лицах (исключая работников Банка), которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ, о перечне обрабатываемых персональных данных и источнике их получения, о сроках обработки персональных данных, в том числе о сроках их хранения;
- отозвать согласие на обработку персональных данных, в случае если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- требовать изменения, уточнения персональных данных, если информация является неполной, недостоверной или устаревшей, или уничтожения информации о самом себе, если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде;
- определять представителей для решения всех вопросов об обработке своих персональных данных.

4. Особенности обработки персональных данных на бумажных носителях

4.1. При обработке персональных данных на бумажных носителях запрещено фиксировать на одном носителе персональные данные, цели обработки которых заведомо не совместимы.

4.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, рекомендуется включать в типовую форму такого документа уведомление субъекта о наличии обработки персональных данных, содержащее необходимую информацию в соответствии с требованиями законодательства Российской Федерации. В случае необходимости получать согласие субъекта на обработку его персональных данных, уведомление об обработке может быть заменено согласием.

4.3. В случае необходимости уточнения персональных данных на бумажном носителе, они фиксируются путем внесения изменений на тот же бумажный носитель либо путем изготовления нового бумажного носителя с уточненными персональными данными и уничтожением старого бумажного носителя.

4.4. Уничтожение или обезличивание части персональных данных может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на бумажном носителе.

5. Особенности предоставления персональных данных

5.1. Наряду с обеспечением конфиденциальности сведений, составляющих персональные данные, Банк предоставляет указанные сведения самому субъекту ПДн или его представителю, а также государственным органам и их должностным лицам, организациям в случаях и в порядке, предусмотренном законодательством Российской Федерации.

5.2. Банк предоставляет на безвозмездной основе сведения, составляющие персональные

данные, государственным органам и их должностным лицам, организациям в рамках их компетенции, определенной законодательством Российской Федерации, при поступлении в Банк оригинала оформленного надлежащим образом мотивированного запроса в письменной форме.
5.3. Доступ к своим персональным данным предоставляется субъекту ПДн или его законному представителю Банком в соответствии с процедурой, описанной в п. 3.2.19 данного Положения.
5.4. Трансграничная передача персональных данных Банком не осуществляется.

6. Требования по организации и обеспечению безопасности персональных данных

6.1. Обеспечение безопасности персональных данных при их обработке в ИСПДн достигается реализацией совокупности организационных и технических мер. В интересах обеспечения безопасности персональных данных защите подлежат технические и программные средства, используемые при обработке персональных данных, а также носители информации.
6.2. Мероприятия по обеспечению безопасности персональных данных формулируются в зависимости от уровня защищенности ИСПДн с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.
6.3. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

- определение уровней защищенности ИСПДн;
- учет работников, допущенных к работе с персональными данными в ИСПДн (определяется «Списком работников ООО Банк Оранжевый, имеющих доступ к персональным данным»);
- определение угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе модели угроз;
- разработку на основе частной (отраслевой) модели угроз требований к построению СЗПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности ИСПДн;
- проверку готовности СЗПДн к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию СЗПДн в соответствии с эксплуатационной и технической документацией;
- описание СЗПДн;
- обучение работников, использующих СЗПДн, применяемые в ИСПДн, правилам работы с ними;
- учет применяемых СЗПДн, эксплуатационной и технической документации к ним, носителей персональных данных;
- контроль соблюдения условий использования СЗПДн, предусмотренных эксплуатационной и технической документацией;
- проведение внутренних проверок (расследований) по выявленным фактам несоблюдения условий хранения носителей персональных данных, использования СЗПДн, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных,

разработка и принятие мер по предотвращению возможных последствий подобных нарушений.

6.4. Доступ к ИСПДн предоставляется на основе заявки [9.2.1].

6.5. Работники Банка, ответственные за обработку и хранение персональных данных, имеющие доступ к персональными данными в силу своих должностных обязанностей, при приеме на работу подписывают «Обязательство о соблюдении требований обращения с конфиденциальной информацией» [9.2.2], за исключением случаев, когда аналогичные требования отражены в трудовом договоре или должностных обязанностях.. Оригиналы подписанных «Обязательств о соблюдении требований обращения с конфиденциальной информацией» хранятся в Отделе по работе с персоналом Банка.

6.6. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в ИСПДн, подлежат учету с использованием индексов (или условных наименований) и регистрационных номеров в Журнале (Приложение 12). Учет ведется работниками ОИБ.

6.7. Для защиты ПДн должны применяться СЗИ, прошедшие процедуру сертификации регулирующими органами (ФСТЭК России, ФСБ и т.д.)

7. Порядок хранения сведений, составляющих персональные данные

7.1. Персональные данные хранятся в ИСПДн, указанных в «Списке систем ООО Банк Оранжевый в которых обрабатываются персональные данные», утвержденном Председателем Правления. Список разрабатывается ОИБ совместно с ОСАиТ.

7.2. Персональные данные на бумажных носителях хранятся в рабочее и нерабочее время в металлических запирающихся шкафах. Во время работы с документами, содержащими персональные данные, допускается хранение таких документов в течение рабочего дня в личных запирающихся шкафах.

7.3. На рабочем столе работника Банка должны находиться только те документы, содержащие персональные данные, с которыми он в настоящий момент работает. Остальные документы, содержащие персональные данные, должны находиться в закрытом на ключ шкафу.

7.4. Хранение персональных данных и носителей ПДн должно осуществляться в форме и объеме, необходимом для целей обработки персональных данных, не дольше, чем обусловлено соответствующими сроками обработки персональных данных. По окончанию срока хранения, персональные данные подлежат уничтожению в установленном порядке, если для продолжения хранения отсутствуют основания, предусмотренные законодательством Российской Федерации.

8. Ответственность за нарушение режима обработки персональных данных

8.1. Все работники Банка, осуществляющие обработку персональных данных, обязаны хранить тайну о сведениях, содержащих персональные данные, в соответствии с требованиями законодательства Российской Федерации, настоящего Положения и внутренними документами Банка.

8.2. В случае если работнику Банка стало известно о факте (попытке) несанкционированного разглашения персональных данных, либо на работника Банка оказывается (оказывалось) давление с целью получения таких сведений, либо в отношении работника Банка производятся (производились) иные действия с целью незаконного получения персональных данных, работник Банка обязан незамедлительно информировать об этом

Председателя Правления Банка, Руководителя Службы внутреннего контроля и лицо (отдел), назначенное ответственным за обеспечение безопасности персональных данных, обрабатываемых в Банке.

8.3. Ответственность за соблюдение мер безопасности при обработке персональных данных, находящихся на рабочих станциях работников Банка, съемных носителях информации и на бумажных носителях информации, возлагается на работников Банка, осуществляющих обработку этих данных.

8.4. Контроль соблюдения требований настоящего Положения возлагается на Отдел информационной безопасности, осуществляется не реже одного раза в год, результаты контроля фиксируются в соответствующем Акте [9.2.3].

9. Нормативные ссылки

9.1. Настоящее Положение разработано на основе следующих законодательных и нормативных документов Российской Федерации, регулирующих правила и требования по обеспечению информационной безопасности персональных данных:

9.1.1. Федерального закона «О персональных данных» от 27 июля 2006 года № 152-ФЗ.

9.1.2. Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9.1.3. 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».

9.1.4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9.1.5. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. (РС БР ИББС-1.0-2014 от 1 июня 2014 года).

9.2. Внутренних документов банка:

9.2.1. Положение о предоставлении прав доступа к автоматизированным системам ООО «ПромСервисБанк».

9.2.2. Положение о защите конфиденциальной информации ООО «ПромСервисБанк».

9.2.3. Регламент повышения осведомленности работников ООО «ПромСервисБанк» в вопросах обеспечения информационной безопасности.

Приложение 1
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример ответа об обработке персональных данных

И.И. Иванову

Уважаемый Иван Иванович

В ответ на Ваш запрос №_____ от _____ сообщаем, что ООО Банк Оранжевый (далее - Банк) осуществляет обработку персональных данных, принадлежащих

_____
(Фамилия, Имя, Отчество)

(далее - Субъект), _____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан

_____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

Обработка ведется на основании _____
_____
(основание для обработки персональных данных)

с использованием средств автоматизации и без использования средств автоматизации с целью заключения с Субъектом любых договоров и их дальнейшего исполнения, принятия решений или совершения иных действий, порождающих юридические последствия в отношения Субъекта и иных лиц, информирования Субъекта о других продуктах, услугах и программах, проводимых Банком.

Персональные данные представлены_____
_____
(источник получения персональных данных)

Срок обработки персональных данных определяется в соответствии со сроком действия _____ с Субъектом персональных данных, сроком исковой давности, нормативными актами Банка России, а также иными требованиями законодательства Российской Федерации. Срок хранения персональных данных определяется Приказом Министерства культуры Российской Федерации от 25.08.2010 №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

Субъект может отозвать согласие на обработку персональных данных путем направления в Банк заявления об отзыве Согласия Субъекта персональных данных, составленного в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Банком обрабатываются персональные данные следующих типов:
_____
(адрес фактического проживания; контактные данные; сведения об образовании; сведения о трудовой деятельности; прочие сведения)

Уполномоченное лицо _____ /_____

Приложение 2
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример ответа об отсутствии обработки персональных данных

И.И. Иванову

Уважаемый Иван Иванович

В ответ на Ваш запрос №_____ от _____ сообщаем, что ООО Банк Оранжевый не осуществляет обработку персональных данных, принадлежащих

_____
(Фамилия, Имя, Отчество)

_____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан _____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

Уполномоченное лицо _____ /_____ /

Приложение 3
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример ответа об отказе в предоставлении информации о наличии обработки персональных данных

И.И. Иванову

Уважаемый Иван Иванович

В ответ на Ваш запрос №_____ от _____ ООО Банк Оранжевый (далее – Банк) сообщает, что в соответствии с

_____
(причина отказа в предоставлении информации*)

_____
_____
_____
_____

Таким образом, Банк не имеет предусмотренных законодательством Российской Федерации оснований на представление информации о наличии обработки персональных данных принадлежащих

_____
(Фамилия, Имя, Отчество)

_____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан_____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

Председатель Правления _____ /_____ /

_____

*Возможные причины отказа:
1. ч. 4 ст. 14 Федерального закона «О персональных данных»: тридцатидневный срок, установленный между повторными запросами об обработке персональных данных, не истек.
2. ч. 5 ст. 14 Федерального закона «О персональных данных»: повторный запрос не содержит достаточного обоснования, для направления такого запроса.
3. ч. 8 ст. 14 Федерального закона «О персональных данных»: Банк имеет право ограничить доступ субъекта к персональным данным на основании того, что обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.
4. ч. 8 ст. 14 Федерального закона «О персональных данных»: Банк имеет право ограничить доступ субъекта к персональным данным на основании того, что доступ субъекта нарушает права и законные интересы третьих лиц.

Приложение 4
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример уведомления о наличии обработки персональных данных

И.И. Иванову

Уважаемый Иван Иванович

Уведомляем Вас о том, что ООО Банк Оранжевый (далее – Банк), расположенный по адресу г. Санкт-Петербург, ул. Рузовская, д. 16, лит А проводит обработку Ваших персональных данных, представленных

_____

(источник получения персональных данных)

_____

Персональные данные обрабатываются с целью_____

(цель обработки персональных данных)

_____

Обработка ведется на основании федеральных законов «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансировании терроризма», нормативных актов Банка России, иных нормативных правовых актов.

К обрабатываемым персональным данным могут иметь доступ уполномоченные работники Банка

Вы имеете право:

- ознакомиться со своими персональными данными, обрабатываемыми Банком;
- получить информацию о способах, правовых основаниях и целях обработки персональных данных, о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ, о перечне обрабатываемых персональных данных и источнике их получения, о сроках обработки персональных данных, в том числе о сроках их хранения;
- отозвать согласие на обработку персональных данных, в случае если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- требовать изменения, уточнения персональных данных, если информация является неполной, недостоверной или устаревшей или уничтожения информации о самом себе, если персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки;
- обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде;
- определять представителей для решения всех вопросов об обработке своих персональных данных.

Уполномоченное лицо _____ /_____ /

Приложение 5
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример уведомления о внесении изменений в некорректные персональные данные

И.И. Иванову

Уважаемый Иван Иванович

Уведомляем Вас о том, что на основании запроса о внесении изменений в некорректные персональные данные, принадлежащие

_____
(Фамилия, Имя, Отчество)

_____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан _____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

были внесены следующие изменения:

1. …заменено на ….
2. …заменено на ….
3. …заменено на ….*

Уполномоченное лицо _____ /_____ /

_____

* Формат описания внесенных изменений.
1. Дата рождения «07.09.1976» заменена на «09.09.1976».
2. Отчество «Иванович» заменено на «Петрович»

Приложение 6
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример письма о внесении изменений в переданные персональные данные

И.И. Иванову

Уважаемый Иван Иванович

Просим Вас внести изменения в переданные_____
(наименование организации)

на основании_____
(правовые основания передачи персональных данных)

персональные данные, принадлежащие

_____
(Фамилия, Имя, Отчество)

_____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан _____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

были внесены следующие изменения:

1. …заменено на ….
2. …заменено на ….
3. …заменено на ….*

Уполномоченное лицо _____/_____/

_____
* Формат описания внесенных изменений.
1. Дата рождения «07.09.1976» заменена на «09.09.1976».
2. Отчество «Иванович» заменено на «Петрович»

Приложение 7
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример уведомления о проведенных мероприятиях по факту обнаружения неправомерной обработки персональные данные

И.И. Иванову

Уважаемый Иван Иванович

Уведомляем Вас о том, что на основании запроса об удалении _____
_____
(незаконно полученных персональных данных, персональных данных не являющихся необходимыми для заявленных целей обработки персональных данных)
принадлежащих

_____
(Фамилия, Имя, Отчество)

_____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан _____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

ООО Банк Оранжевый проведены мероприятия по _____

_____
(обеспечению правомерности обработки персональных данных/удалению этих персональных данных из информационных систем Банка)

Уполномоченное лицо _____/_____/

Приложение 8
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Пример письма об удалении персональных данных

И.И. Иванову

Уважаемый Иван Иванович

Просим удалить переданные_____
(наименование организации)

на основании_____
(правовые основания передачи персональных данных)

персональные данные, принадлежащие

_____
(Фамилия, Имя, Отчество)

_____ серия _____ номер _____
(наименование документа, удостоверяющего личность)

выдан _____
(дата выдачи) (наименование органа, выдавшего документ, удостоверяющий личность)

в связи с _____
(выявлением факта незаконности их получения/избыточностью для заявленных целей обработки персональных данных)

Уполномоченное лицо _____/_____/

Приложение 9
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

УТВЕРЖДАЮ
Председатель Правления
ООО Банк Оранжевый

_____/_____
«___»_____201__г

Акт удаления персональных данных

Комиссия в составе:

Председатель _____

Члены комиссии _____
_____
_____

провела отбор записей субъектов персональных данных в информационных системах обработки персональных данных с использованием средств автоматизации (далее - ИСПДН), цель обработки персональных данных которых утрачена и/ или срок хранения информации истек.
Всего выявлено _____ записей в следующих ИСПДН:

№ п/п	Субъект ПДн	Наименование ИСПДн	Количество выявленных записей	Примечание

Согласно требованию законодательства Российской Федерации и «Положению о порядке обработки персональных данных в ООО Банк Оранжевый указанные записи были удалены путем_____
_____

Председатель комиссии: _____/_____/

Члены комиссии: _____/_____/

_____/_____/

_____/_____/

Приложение 10
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

УТВЕРЖДАЮ
Председатель Правления
ООО Банк Оранжевый

_____/_____
«___»_____201__г

Акт уничтожения носителей персональных данных

Комиссия в составе:

Председатель _____

Члены комиссии _____
_____
_____

провела отбор носителей персональных данных (далее - ПДн) и установила, что в соответствии с требованиями законодательства Российской Федерации и «Положению о порядке обработки персональных данных в ООО Банк Оранжевый» информация, записанная на них в процессе использования, подлежит гарантированному уничтожению.

Всего отобрано _____ носителей ПДн:

№ п/п	Субъект ПДн	Тип носителя	Регистрационный номер носителя ПДн	Примечание

На указанных носителях персональные данные уничтожены путем_____
(удаления на устройстве гарантированного уничтожения информации и т. д.)

Перечисленные носители ПДн уничтожены путем_____
_____
(разрезания, сжигания, механического уничтожения, сдачи предприятию по утилизации вторичного сырья и т.д.)

Председатель комиссии: _____/_____/

Члены комиссии: _____/_____/
_____/_____/
_____/_____/

Приложение 11
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Журнал учета обращений субъектов персональных данных (законных представителей субъектов персональных данных), уполномоченного органа по защите прав субъектов персональных данных.

Журнал начат
«____» _____201__г.
_____
(должность)
_____/_____
(Фамилия, инициалы и подпись должностного лица)

Журнал завершен
«____» _____201__г.
_____
(должность)
_____/_____
(Фамилия, инициалы и подпись должностного лица)

Общие количество листов _____*

№ п/п	Дата поступления запроса	Сведения о запрашивающем лице	Сведения о запрашиваемом лице	Цель запроса	Отметка о предоставлении информации или отказе в ее предоставлении	Дата ответа на запрос	Подпись работника	Примечание
1	2	3	4	5	6	7	8	9

Приложение 12
к Положению о порядке обработки персональных данных в ООО Банк Оранжевый

Журнал учета средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в ИСПДн.

Журнал начат
«____» _____201__г.
_____
(должность)
_____/_____
(Фамилия, инициалы и подпись должностного лица)

Журнал завершен
«____» _____201__г.
_____
(должность)
_____/_____
(Фамилия, инициалы и подпись должностного лица)

Общие количество листов _____*

№ п/п	Наименование СЗИ	Место установки	Наименование ИСПДн	Дата ввода в эксплуатацию, подпись администратора СЗИ	Дата вывода из эксплуатации, подпись администратора СЗИ	Примечание
1	2	3	4	5	6	9