УТВЕРЖДЕНО

Решением Правления

Протокол № 10 от 19 августа 2022г.

ПОЛОЖЕНИЕ
О ПОРЯДКЕ И УСЛОВИЯХ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АО «СМБСР БАНК»

Москва, 2022

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение разработано в целях соответствия требованиям законодательства о защите персональных данных (Федеральному закону №152-ФЗ «О персональных данных», соответствующим постановлениям Правительства, применимым актам органов государственной власти), а также нормативным актам и актуальным Стандартам информационной безопасности Банка России в части защиты персональных данных

1.2. Положение устанавливает основные понятия, цели и основания обработки персональных данных, объем и категории персональных данных и их субъектов, порядок и условия обработки персональных данных, меры по обеспечению безопасности персональных данных при их обработке и иные аспекты, касающиеся персональных данных.

Отдельные вопросы, касающиеся процесса и принципов обработки ПД, также могут содержаться в иных внутренних документах Банка, но не должны противоречить требованиям и принципам настоящего Положения.

1.3. Основные понятия, используемые в настоящем Положении:

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники. Обработка ПД, содержащихся в ИСПДН либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации, если такие действия с ПД, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

Банк – Акционерное общество «Сумитомо Мицуи Рус Банк», включено в реестр операторов персональных данных под номером 09-0076585 в соответствии с требованиями Федерального закона №152-ФЗ от 27.07.2006г.;

Бенефициары – выгодоприобретатели и бенефициарные владельцы, лица, осуществляющие контроль, устанавливаемые Банком в целях соблюдения требований действующего законодательства и положениями внутренних документов Банка;

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

Информационная система персональных данных (ИСПДН) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Кадровое подразделение – Департамент управления человеческими ресурсами;

Клиент – лицо, находящееся на обслуживании в Банке с целью получения банковских услуг, иных финансовых продуктов и услуг, оказываемых Банком в соответствии с лицензией и Уставом, и/или заключения банковских сделок (включая кредитные организации и лиц, обращающихся в Банк для принятия на обслуживание и представляющих для этого документы в соответствии с действующим законодательством и внутренними документами Банка);

Контрагент – любое лицо, с которым Банк осуществляет деловое сотрудничество (либо находится в стадии переговоров о таком сотрудничестве и рассматривает документы, необходимые для такого сотрудничества), в том числе, у которого приобретает товары, продукты, работы, услуги на основании любых контрактов, договоров, соглашений, счетов, публичных оферт и иных законных основаниях (за исключением лиц, состоящих с Банком в трудовых отношениях, а также лиц, являющихся Клиентами);

Конфиденциальность персональных данных – режим ограниченного доступа к персональным данным, обеспечивающий их защиту и обработку в соответствии с требованиями действующего законодательства, в частности запрещающий Операторам ПД раскрывать третьим лицам и распространять ПД без согласия Субъекта ПД, если иное не предусмотрено федеральным законом;

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

Обработка персональных данных (Обработка ПД) – любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка ПД включает в себя, в том числе: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

Оператор – оператор персональных данных, а именно: государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Органы управления – члены Наблюдательного Совета (кандидаты в члены), а также лица, осуществляющие контроль в отношении Банка и его акционеров, не являющиеся работниками Банка;

Персональные данные (ПД) – 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;

Представители – лица, уполномоченные осуществлять действия от имени Клиентов, Контрагентов, в том числе сотрудники, информацию о которых Клиенты, Контрагенты передают в Банк;

Работник (сотрудник) – физическое лицо, связанное с Банком трудовыми отношениями на основании трудового договора;

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

Роскомнадзор – уполномоченный орган по защите прав субъектов персональных данных;

Субъект персональных данных (Субъект ПД) – физическое лицо, прямо или косвенно определенное или определяемое с использованием ПД;

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Федеральный закон (ФЗ) – Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

1.4. Банк руководствуется следующими принципами обработки ПД:

- обработка ПД должна осуществляться на законной и справедливой основе;
- обработка ПД должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПД, несовместимая с целями сбора персональных данных.
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- обработке подлежат только персональные данные, которые отвечают целям их обработки.
- содержание и объем обрабатываемых ПД должны соответствовать заявленным целям обработки. Обрабатываемые ПД не должны быть избыточными по отношению к заявленным целям их обработки.
- при обработке ПД должны быть обеспечены точность ПД, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПД. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
- хранение ПД должно осуществляться в форме, позволяющей определить Субъекта ПД, не дольше, чем этого требуют цели обработки ПД, если срок хранения ПД не установлен федеральным

законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые ПД подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

2. ПРАВА И ОБЯЗАННОСТИ

2.1. Субъект ПД, а также Оператор ПД, обладают как правами, так и обязанностями, связанными с ПД. Выполнение таких обязанностей и соблюдение прав является ключевым элементом, обеспечивающим соблюдение требований Федерального закона, а также иных нормативных актов, регламентирующих обработку ПД.

2.2. Субъект ПД наделен следующими основными правами:

2.2.1. Право на его доступ к ПД.

Субъект ПД имеет право на получение сведений, указанных в ч.7 ст.14 Федерального закона, за исключением случаев, предусмотренных ч.8 указанной статьи. Субъект ПД вправе требовать от Оператора уточнения его ПД, их блокирования или уничтожения в случае, если ПД являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Кроме того, Субъект имеет право на повторный запрос на получение указанных сведений с соблюдением сроков, установленных Федеральным законом.

Право Субъекта ПД на доступ к ПД может быть ограничено только в соответствии с федеральными законами, устанавливающими такое ограничение при соблюдении условий, указанным в ч.8 ст.14 Федерального закона.

2.2.2. Право на обеспечение надлежащей защиты ПД.

Оператор ПД должен обеспечить соблюдение конфиденциальности ПД согласно требованиям Федерального закона.

2.2.3. Право на обжалование действия или бездействия Оператора.

Если Субъект ПД считает, что Оператор осуществляет обработку его ПД с нарушением требований Федерального закона или иным образом нарушает его права и свободы, Субъект ПД вправе обжаловать действия или бездействие оператора, обратившись в Роскомнадзор или в судебном порядке.

2.2.4. Право на возмещение убытков.

Субъект ПД имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда, возникших в результате нарушений при обработке его ПД, в судебном порядке.

2.2.5. Право на соблюдение Оператором законодательно закрепленных ограничений на Обработку ПД, установленных в интересах Субъекта ПД.

В тех случаях, когда Федеральный закон устанавливает необходимость получения согласия Субъекта ПД на обработку ПД, такая обработка может производиться исключительно при условии получения Оператором такого согласия.

Указанный выше перечень прав содержит упоминание наиболее базовых прав и не является исчерпывающим. Субъект ПД обладает всеми правами, закрепленным действующим законодательством.

2.3. Субъект ПД обязан:

2.3.1. Реализовывать свои права разумно, с должной степенью осмотрительности и добросовестности, в частности, избегать злоупотребления своими правами в целях совершения противоправных действий;

2.3.2. Соблюдать действующее законодательство, включая Федеральный закон.

2.4. Банк как Оператор ПД наделен следующими основными правами:

2.4.1. Осуществлять обработку ПД в случаях, установленных ст.6 Федерального закона.

2.4.2. Поручать обработку данных ПД другому лицу в случаях и на условиях, установленных Федеральным законом.

2.4.3. В случаях, установленных Федеральным законом, осуществлять обработку ПД после отзыва Субъектом ПД своего согласия на Обработку ПД.

2.4.4. Получать ПД от лица, не являющегося Субъектом ПД, в случаях, установленных Федеральным законом.

2.4.5. Отказать Субъекту ПД в выполнении повторного запроса о предоставлении доступа к ПД в случаях, установленных Федеральным законом.

Указанный выше перечень прав не является исчерпывающим. Оператор ПД обладает всеми правами, закрепленным действующим законодательством.

2.5. Основные обязанности Банка как Оператора ПД:

2.5.1. Не раскрывать третьим лицам и не распространять ПД без согласия субъекта персональных данных, если иное не предусмотрено соответствующим федеральным законом.

2.5.2. При Трансграничной передаче ПД убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПД, обеспечивается адекватная защита прав Субъектов ПД, до начала осуществления трансграничной передачи ПД.

2.5.3. Прекратить обработку ПД по требованию Субъекта ПД за исключением случаев, напрямую установленных Федеральным законом.

2.5.4. Предоставить доступ к ПД Субъекту ПД по его запросу, запросу его Представителя, а также предоставлять информацию Роскомнадзору по его запросу.

2.5.5. Разъяснять Субъекту ПД порядок принятия решения на основании исключительно автоматизированной обработки его ПД и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, рассмотреть его, а также разъяснить порядок защиты Субъектом ПД своих прав и законных интересов.

2.5.6. При сборе ПД Оператор ПД обязан предоставить Субъекту ПД по его просьбе информацию, предусмотренную ч. 7 ст. 14 Федерального закона.

2.5.7. Если предоставление ПД и (или) получение Оператором согласия на обработку ПД являются обязательными в соответствии с Федеральным законом, Оператор обязан разъяснить Субъекту ПД юридические последствия отказа предоставить ПД и (или) дать согласие на их обработку.

2.5.8. Если ПД получены не от Субъекта ПД, Оператор, за исключением случаев, предусмотренных ч. 4 ст.18, до начала обработки таких ПД обязан предоставить информацию в объеме, установленном Федеральным законом, за исключением случаев, когда Оператор освобожден от такой обязанности Федеральным законом.

2.5.9. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, в том числе для защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПД, а также от иных неправомерных действий в отношении ПД.

2.5.10. Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПД согласно требованиям Федерального закона, к сведениям о реализуемых требованиях к защите ПД.

2.5.11. Предоставлять документы, определяющие меры необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, по запросу Роскомнадзора.

2.5.12. В случае, если для Обработки ПД необходимо согласие Субъекта ПД, Оператор обязан получить такое согласие до начала Обработки ПД.

2.5.13. Не позднее 7 рабочих дней со дня представления Субъектом ПД или его Представителем сведений, подтверждающих, что такие ПД являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уничтожить такие ПД, после чего уведомить Субъекта ПД о принятых мерах и изменениях, а также принять разумные меры для уведомления третьих лиц.

2.5.14. Устранять нарушения законодательства, допущенные при Обработке ПД, по уточнению, блокированию и уничтожению персональных данных в соответствии со ст.21 Федерального закона.

2.5.15. Обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПД.

Указанный выше перечень обязанностей не является исчерпывающим. Оператор ПД обязан осуществлять все необходимые действия, требуемые действующим законодательством.

3. ЦЕЛИ ОБРАБОТКИ ПД И КАТЕГОРИИ СУБЪЕКТОВ ПД

3.1. Обработка ПД должна ограничиваться достижением конкретных, заранее определенных и законных целей, в частности не допускается обработка ПД, несовместимая с целями сбора ПД.

3.2. Содержание и объем обрабатываемых ПД должны соответствовать заявленным целям обработки. Обрабатываемые ПД не должны быть избыточными по отношению к заявленным целям их обработки. Обработке подлежат только ПД, которые отвечают целям их обработки.

3.3. Не допускается объединение баз данных, содержащих ПД, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Банк обрабатывает ПД (в том числе в ИСПДН) в целях:

1) исполнения Банком обязанностей, налагаемых действующим законодательством (включая, но не ограничиваясь, представление обязательной отчетности, реализации мер ПОД/ФТ/ФРОМУ, ведения налогового учета, удержаний из заработной платы в случаях, установленных законодательством, международного обмена налоговой информацией, исполнения требований нормативных актов Банка России, требований Трудового кодекса, соблюдения санитарных и санитарно-эпидемиологических норм и требований),

2) осуществления банковских операций и иных сделок, оказания иных финансовых услуг, предусмотренных Уставом Банка, законодательством Российской Федерации, нормативными актами Банка России, лицензиями,

3) заключения, исполнения и прекращения Банком договоров, контрактов, соглашений с Клиентами и Контрагентами,

4) ведения кадрового делопроизводства, реализации трудовой деятельности, включая исполнения должностных обязанностей сотрудниками, мотивации и обучения персонала, содействия работникам в трудоустройстве, получения образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества,

5) иных целях, предусмотренных действующим законодательством, настоящим Положением, Перечнем ПД, обрабатываемых Банком, и согласиями Субъектов ПД.

3.5. Правовыми основаниями для обработки ПД является совокупность нормативных правовых актов Российской Федерации, применимых к деятельности Банка, среди которых наиболее значимыми являются:

- Федеральный закон «О банках и банковской деятельности» № 395-1 от 02.12.1990г.;
- Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» № 115-ФЗ от 07.08.2001г.;
- Федеральный закон «О судебных приставах» № 118-ФЗ от 21.07.1997г.;
- Федеральный закон «О кредитных историях» № 218-ФЗ от 30.12.2004г.;
- Трудовой кодекс РФ;
- Налоговый кодекс РФ;
- Положение Банка России № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма» от 15.10.2015г.;
- Инструкция Банка России № 153-И «Об открытии и закрытии банковских счетов, счетов по вкладам, депозитных счетов» от 30.05.2014г. (с 01.10.2022 – Инструкция Банка России №204-И «Об открытии, ведении и закрытии банковских счетов и счетов по вкладам (депозитам)» от 30.06.2021г.)

Кроме того, к правовым основаниям Банк относит Устав в действующей редакции, выданные Банку лицензии, договоры, контракты, соглашения с Субъектами ПД, а также согласия на обработку ПД (в случаях, прямо не предусмотренных законодательством, но соответствующих деятельности Банка).

3.6. К категориям Субъектов ПД, чьи ПД может обрабатывать Банк, относятся, в том числе:

1) Работники (сотрудники) Банка, бывшие работники, кандидаты на замещение вакантных должностей, а также родственники работников (в случаях, когда это необходимо по требованию законодательства, либо по просьбе Работника), лица, являющиеся работниками и входящие в Органы управления;

2) Клиенты и Контрагенты Банка;

3) Представители Клиентов и Контрагентов;

4) Органы управления.

В рамках каждой из категорий Субъектов ПД и применительно к конкретным целям Банк определяет обрабатываемые ПД и случаи обработки ПД в отдельном Перечне ПД, обрабатываемых Банком, с указанием лиц, имеющих к ним доступ.

В случае возникновения необходимости, соответствующей целям Обработки ПД, указанным в разделе 3, Банк имеет право обрабатывать ПД и иных категорий Субъектов ПД, напрямую не поименованных в настоящем пункте, при условии соблюдения требований Федерального закона.

4. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПД

4.1. Банк осуществляет следующие меры по обеспечению безопасности ПД при их обработке:

1) исключение несанкционированного, в том числе случайного, доступа к ПД, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПД, а также иных несанкционированных действий;

2) определение круга лиц, имеющих доступ к ПД и/или участвующих в их обработке и назначение лица, ответственного за обеспечение безопасности персональных данных;

3) в случае хранения или обработки ПД в электронном виде использование технических средств и технологии обеспечения защиты ПД, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПД);

4) хранение носителей, содержащих ПД, в защищенном месте, недоступном для лиц, не входящих в число лиц, допущенных к работе с ПД;

5) наличие модели угроз информационной безопасности;

6) управление доступом к средствам вычислительной техники (СВТ), программам и данным;

7) обеспечение антивирусной защиты ПД, хранящихся в электронном виде;

8) ПД при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях ПД;

9) сохранность ПД, хранящихся в электронном виде, обеспечивается путем их резервного копирования.

Под техническими средствами, позволяющими осуществлять обработку ПД, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

4.2. Мероприятия Банка по обеспечению безопасности ПД при их обработке в информационных системах включают в себя:

а) определение угроз безопасности ПД при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПД, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПД, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей ПД;

ж) учет лиц, допущенных к работе с ПД в информационной системе и вне её;

з) контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПД, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) ограничение круга лиц, имеющих доступ к ПД;

л) лица, обрабатывающие ПД, должны быть уведомлены об этом.

Перечень мер по обеспечению безопасности ПД определяется настоящим Положением и является минимально необходимым. Банк оставляет за собой право применять иные не запрещенные законом меры, не упомянутые в настоящем Положении, в случае если это требуется для обеспечения безопасности ПД.

4.3. Лицо, ответственное за обеспечение безопасности персональных данных, в случае возникновения угрозы безопасности незамедлительно предоставляет Правлению информацию о её текущем состоянии.

4.4. В Банке запрещается:

1) хранение в открытом доступе документов на бумажном носителе в случае, если они содержат ПД;

2) хранение и обработка ПД без согласия субъекта ПД (если такое согласие не требуется в силу Федерального закона);

3) привлечение сотрудников Банка к обработке ПД без уведомления их об этом;

4) предоставление ПД (доступа к ПД) или распространение ПД без получения согласия Субъекта ПД (за исключением случаев, когда таковое не требуется согласно Федеральному закону).

5. УСЛОВИЯ ДОСТУПА К ПД

5.1. Допуск к ПД (как сотрудников Банка, так и иных Субъектов, предоставивших в Банк свои ПД), допускается при условии, что такой доступ разрешен распорядительным актом, либо иным внутренним документом Банка.

5.2. Допуск к ПД может быть предоставлен исключительно в целях:

1) исполнения Банком обязанностей, налагаемых действующим законодательством (включая, но не ограничиваясь, представление обязательной отчетности, реализации мер ПОД/ФТ/ФРОМУ, ведения налогового учета, удержаний из заработной платы в случаях, установленных законодательством, международного обмена налоговой информацией),

2) осуществления банковских операций и иных сделок, оказания иных финансовых услуг, предусмотренных Уставом Банка, законодательством Российской Федерации, нормативными актами Банка России, лицензиями,

3) заключения, исполнения и прекращения Банком договоров, контрактов, соглашений с Клиентами и Контрагентами,

4) ведения кадрового делопроизводства, реализации трудовой деятельности, включая исполнения должностных обязанностей сотрудниками, мотивации и обучения персонала, содействия работникам в трудоустройстве, получения образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества,

5) иным целям, предусмотренным действующим законодательством, настоящим Положением, Перечнем ПД, обрабатываемых Банком, и согласиями Субъектов ПД.

5.3. Банк систематизирует обработку ПД в целях разграничения доступа к ПД и контроля:

1) в отношении ПД Представителей и Бенефициаров Клиентов, Клиентов (далее ПД Клиентов) в разрезе юридических досье Клиентов и в отношении ПД лиц, представителей Клиентов, которые ещё не приняты на обслуживание в разрезе временных файлов юридических лиц.

В случае отказа Клиента либо Банка от принятия на обслуживание ПД из временного файла юридического лица подлежат уничтожению в связи с достижением цели обработки в срок, установленный законодательством;

2) в отношении ПД работников и их родственников (включая бывших сотрудников) в разрезе личных папок работников Банка, а также папок хранения соответствующей документации Кадрового подразделения (по типам документов).

В случае принятия решения о найме кандидата по нему формируется личная папка работника. ПД, не подлежащие включению в личную папку работников, подлежат уничтожению в установленный Федеральным законом срок.

В случае отказа от найма кандидата все ПД по нему также подлежат уничтожению в установленный Федеральным законом срок.

В целях ограничения числа лиц, имеющих непосредственный доступ к таким ПД, а также контроля за сохранностью ПД, ответственным за хранение и уничтожение ПД данной категории является Кадровое подразделение.

Трудовые книжки (оригиналы) Работников учитываются в книге движения трудовых книжек согласно требованиям трудового законодательства, при увольнении Работника трудовая книжка подлежит возврату Работнику. При переходе Банка на ведение трудовых книжек в электронном виде в установленный законодательством срок бумажные трудовые книжки подлежат передаче Работникам, если иное не будет предусмотрено действующим законодательством.

3) в отношении ПД Органов управления (за исключением являющихся сотрудниками Банка) в разрезе папки по деловой репутации, а также в составе обязательной отчетности, представленной в Банк России;

4) в отношении ПД Контрагентов и их Представителей в составе договоров, соглашений, контрактов с Контрагентам;

5) в отношении ПД, разрешенных субъектом ПД для распространения, в том числе для публикации в сети Интернет в соответствии с требованиями по раскрытию информации, в составе блоков раскрываемой информации.

5.4. При обнаружении нарушений порядка предоставления ПД Банк или уполномоченное лицо незамедлительно приостанавливают доступ к ПД пользователям информационной системы до выявления причин нарушений и устранения этих причин.

5.5. Сотрудники Банка имеют доступ к ПД исключительно в объеме, необходимом для осуществления ими своих должностных обязанностей. Должностные лица, имеющие доступ к конкретной категории ПД, объем и состав ПД разных категорий, определены в Перечне ПД, утверждаемом приказом Президента Банка.

Разграничение доступа к ПД в информационных системах реализуется путем разграничения доступа к информационным системам и файловым папкам, который предоставляется строго в соответствии с должностными обязанностями Работников на основании запроса в системе, одобряемого руководством Банка.

Разграничение доступа к материальным носителям ПД обеспечивается хранением материальных носителей в различных местах в запираемых шкафах и сейфах, доступ к содержимому

которых имеют только лица, участвующие в обработке данной категории ПД для конкретной цели обработки.

5.6. Лица, осуществляющие обработку ПД без использования средств автоматизации подлежат информированию о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПД

6.1. Методы и способы обработки ПД должны соответствовать целям, обозначенным в согласиях на обработку ПД, предоставляемых субъектами ПД (в случаях, когда такое согласие требуется в силу требований законодательства).

6.2. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПД (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения ПД, сроки обработки ПД, перечень действий с ПД, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПД;

б) типовая форма должна предусматривать поле, в котором Субъект ПД может поставить отметку о своем согласии на обработку ПД, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку ПД;

в) типовая форма должна быть составлена таким образом, чтобы каждый из Субъектов ПД, содержащихся в документе, имел возможность ознакомиться со своими ПД, содержащимися в документе, не нарушая прав и законных интересов иных Субъектов ПД;

г) типовая форма должна исключать объединение полей, предназначенных для внесения ПД, цели обработки которых заведомо не совместимы.

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

При несовместимости целей обработки ПД, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку ПД отдельно от других зафиксированных на том же носителе ПД, Банк принимает меры по обеспечению раздельной обработки ПД, в частности:

а) при необходимости использования или распространения определенных ПД отдельно от находящихся на том же материальном носителе других ПД осуществляется копирование ПД, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПД, не подлежащих распространению и использованию, и используется (распространяется) копия ПД;

б) при необходимости уничтожения или блокирования части ПД уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПД, подлежащих уничтожению или блокированию.

6.4. Машинные носители ПД (если таковые имеются) подлежат учету в Журнале учета машинных носителей ПД (Приложение 3) и хранению в запираемом помещении с ограниченным доступом.

Учету подлежат только те машинные носители, на которые фактически записаны ПД, а не все машинные носители, которые технически позволяют осуществить запись ПД.

Все машинные носители ПД классифицируются в следующие 3 категории:

съемные машинные носители ПД (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

портативные вычислительные устройства, имеющие встроенные носители ПД (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);

машинные носители ПД, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Журнал учета машинных носителей ПД ведется Службой комплаенс-контроля.

Согласно требованиям информационной безопасности сотрудники Банка по общему правилу не имеют технической возможности осуществлять запись данных на съемные машинные носители. Запись на машинные носители может быть реализована по специальному запросу с помощью сотрудников Службы информационной безопасности. При поступлении такого запроса Служба информационной безопасности информирует Службу комплаенс-контроля. В случае, если записываемая информация содержит ПД, Служба комплаенс-контроля фиксирует информацию в Журнале учета машинных носителей.

6.5. Правила, предусмотренные пунктами 6.2 и 6.3 настоящего Положения, применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе ПД и информации, не являющейся ПД.

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

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

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

6.9. Банк обеспечивает раздельное хранение ПД (материальных носителей), обработка которых осуществляется в различных целях:

1) ПД Представителей и Бенефициаров Клиентов Банка хранятся в досье клиента (юридических делах) в соответствии с требованиями Федерального закона №115-ФЗ и Инструкции Банка России №153-И / №204-И. Досье размещаются в сейфовой комнате Банка, доступ в которую ограничен, в запираемых на ключ шкафах.

ПД Представителей и Бенефициаров Клиентов Банка, с которыми ещё не установлены договорные отношения, но которые представили соответствующие документы для их установления хранятся (до формирования из них досье Клиента либо до отзыва документов Клиентом (по причине непринятия на обслуживание по инициативе Банка либо по желанию Клиента) либо до их уничтожения документов по просьбе Клиента (в случае непринятия на обслуживание) в запираемом металлическом сейфе временного хранения, находящемся в сейфовой комнате, доступ в которую ограничен. Лица, которые могу получать данную информацию, указаны в Перечне ПД;

2) ПД Работников (сотрудников), их родственников, кандидатов на вакантные должности, бывших сотрудников Банка хранятся в запираемых шкафах, непосредственный доступ к содержимому которых имеют только сотрудники Кадрового подразделения, которые расположены в помещении с ограниченным доступом (за исключением ПД разрешенных Субъектом ПД к распространению, которые хранятся и обрабатываются с учетом особенностей, установленных для указанному типу ПД). Трудовые книжки учитываются в книге и их оригиналы подлежат хранению в запираемом шкафу, расположенном в сейфовой комнате. Иные лица, которые могу получать данную информацию указаны в Перечне ПД;

3) ПД членов Органов Управления Банка, не являющихся сотрудниками Банка, полученные в целях исполнения требований законодательства и предоставления в Банк России, хранятся Юридической службой в составе соответствующей отчетности, а также в досье для подтверждения соответствия требованиям к деловой репутации и квалификации, в запираемом шкафу, под контролем Юридической службы, которая имеет непосредственный доступ к указанным документам (за исключением ПД разрешенных Субъектом ПД к распространению, которые хранятся и обрабатываются с учетом особенностей, установленных для указанному типу ПД). Иные лица, которые могу получать данную информацию, указаны в Перечне ПД;

4) ПД Представителей Контрагентов и Контрагентов хранятся в составе договоров, контрактов, соглашений и прилагаемых к ним документов в сейфовой комнате, доступ в которую ограничен в запираемых шкафах под контролем Административного отдела. Иные лица, которые могут получать данную информацию указаны в Перечне ПД.

По общему правилу, если иное не следует из целей обработки ПД, цель обработки ПД является достигнутой по истечении срока хранения документов, содержащих ПД. Сроки хранения документов определяются на основании Приказа Росархива от 20.12.2019 №236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения", Положения Росархива №1, Банка России №801-П от 12.07.2022 "Об утверждении Перечня документов, образующихся в процессе деятельности кредитных организаций, с указанием сроков их хранения", положений Трудового кодекса (в отношении Работников), положений миграционного законодательства, Федерального закона №115-ФЗ и внутренних документов Банка, устанавливающих сроки хранения документов, образующихся в деятельности Банка.

6.10. Безопасность ПД при их обработке в информационной системе обеспечивает Банк или лицо, которому на основании договора оператор поручает обработку персональных данных (далее - уполномоченное лицо). При заключении договора/контракта Юридическая служба Банка и/или Департамент юридической поддержки и комплаенс-контроля проверяет наличие условия об обеспечении конфиденциальности персональных данных и безопасности персональных данных при их обработке.

6.11. При обработке ПД в информационных системах обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к ПД;

в) недопущение воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль над обеспечением уровня защищенности персональных данных.

6.12. Передача ПД Банком третьему лицу осуществляется с согласия субъекта персональных данных, за исключением случаев, когда получение согласия не требуется в соответствии с положениями действующего законодательства. В том случае, если Банк поручает обработку ПД третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности,

6.13. Обезличивание ПД при их обработке осуществляется в случае наличия такой возможности и в случае, если это не противоречит целям и порядку их обработки.

6.14. Банк зарегистрирован в качестве оператора ПД и обязан уведомлять Роскомнадзор об изменениях первоначально заявленных сведений.

6.15. В случае выявления недостоверных ПД или неправомерных действий с ними Банка при обращении или по запросу субъекта ПД или его законного представителя либо уполномоченного органа по защите прав субъектов ПД Банк обязан осуществить блокирование ПД, относящихся к соответствующему субъекту ПД, с момента такого обращения или получения такого запроса на период проверки. В случае подтверждения факта недостоверности ПД Банк на основании документов, представленных ПД данных или его законным представителем либо Роскомнадзором, или иных необходимых документов уточняет ПД и снимает их блокирование.

6.16. В случаях, установленных действующим законодательством, когда Банк обязан раскрывать информацию об Органах Управления, а также иных лицах, выполняющих отдельные функции, обработка особого типа ПД, разрешенных Субъектом ПД к распространению (здесь и далее - ПДРР) осуществляется в соответствии с Федеральным законом, настоящим Положением с учетом особенностей, установленных настоящим пунктом, в частности:

1) согласие на обработку ПДРР оформляется отдельно от иных согласий Субъекта ПД на обработку его ПД. Банк обеспечивает Субъекту ПД возможность определить перечень ПД по каждой категории ПД, указанной в согласии на обработку ПД, разрешенных Субъектом ПД для распространения;

2) в случае, если из предоставленного Субъектом ПД согласия на обработку ПДРР, не следует, что Субъект ПД согласился с распространением ПД, такие ПД обрабатываются Банком без права распространения с учетом всех ограничений на раскрытие указанных данных;

3) в случае, если из предоставленного Субъектом ПД согласия на обработку ПДРР, не следует, что Субъект ПД не установил запреты и условия на обработку персональных данных, предусмотренные Федеральным законом, или если в предоставленном Субъектом ПД согласии не указаны категории и перечень ПД, для обработки которых Субъект ПД устанавливает условия и запреты в соответствии с Федеральным законом, такие ПД обрабатываются Банком без передачи (распространения, предоставления, доступа) и возможности осуществления иных действий с ПД неограниченному кругу лиц;

4) молчание или бездействие Субъекта ПД ни при каких обстоятельствах не может считаться согласием на обработку ПДРР;

5) в согласии на обработку ПД, разрешенных Субъектом ПД для распространения, Субъект ПД вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Банком неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих ПД неограниченным кругом лиц. Отказ Банка в установлении Субъектом ПД запретов и условий, предусмотренных настоящей статьей, не допускается;

6) Банк обязан в срок не позднее трех рабочих дней с момента получения соответствующего согласия Субъекта ПД опубликовать информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц ПД, разрешенных Субъектом ПД.

7) установленные Субъектом ПД запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) ПДРР, не распространяются на случаи обработки ПД в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации;

8) передача (распространение, предоставление, доступ) ПДРР должна быть прекращена в любое время по требованию Субъекта ПД. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) Субъекта ПД, а также перечень ПД, обработка которых подлежит прекращению. Указанные в данном требовании ПД могут обрабатываться только оператором, которому оно направлено;

9) действие согласия Субъекта ПД на обработку ПДРР прекращается с момента поступления Банку требования, указанного в пп.8) настоящего пункта;

10) Субъект ПД вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих ПД, ранее разрешенных им для распространения, к любому лицу, обрабатывающему его ПД, в случае несоблюдения требований Федерального закона или обратиться с таким требованием в суд. Данное лицо обязано прекратить передачу (распространение, предоставление, доступ) ПД в течение трех рабочих дней с момента получения требования Субъекта ПД или в срок, указанный во вступившем в законную силу решении суда, а если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

Любые особенности обработки ПДРР, не указанные в настоящем Положении, определяются в соответствии с требованиями Федерального закона. В случае, если часть ПД, которые Банк обрабатывает в иных целях и на иных основаниях (целях и основаниях, отличных от целей и оснований для которых Субъект ПД предоставил Банку согласие (разрешение) на их

распространение, включая доступ к неограниченного круга лиц) совпадает с ПДРР, то Банк продолжает обработку этой части ПД раздельно и с разными режимами по разным целям и основаниям. Например, если лицо представило согласие на публикацию сведений о полученном образовании на сайте Банка в целях соблюдения требований законодательства о раскрытии информации, Банк публикует указанные ПД на сайте Банка, но при этом продолжает ограничивать доступ к указанным ПД в составе иных документов, представленных Субъектом ПД Банку в иных целях, например, целях трудоустройства.

7. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ БАНКА

7.1. Помимо общих требований и правил обработки ПД, предусмотренных Федеральным законом и настоящим Порядком, Банк устанавливает дополнительные требования к обработке ПД Работников в целях обеспечения соответствия требованиям главы 14 Трудового кодекса («Защита персональных данных работника»).

7.2. Обработка Банком персональных данных Работника осуществляется исключительно в целях:

• обеспечения соблюдения законов и иных нормативных правовых актов;
• содействия работникам в трудоустройстве;
• обеспечения личной безопасности работников;
• контроля количества и качества выполняемой работы;
• обеспечения сохранности имущества работника и работодателя.

Настоящие цели обеспечивают реализацию трудовой деятельности, включая исполнения должностных обязанностей Работниками, получение образования и продвижении по службе, включая мотивацию и обучение, обеспечение личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Банка, • обеспечения личной безопасности работников, включая предоставление сотрудникам дополнительных социальных гарантий, в частности услуг добровольного медицинского страхования.

7.3. Все персональные данные Работника Банк получает у него самого, за исключением случаев, если их получение возможно только у третьей стороны, в этом случае Работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Банк должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

7.4. При определении объема и содержания обрабатываемых ПД Работника Банк руководствуется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

7.5. Банк не имеет права:

- получать и обрабатывать сведения о работнике, относящиеся в соответствии с законодательством Российской Федерации в области ПД к специальным категориям персональных данных, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и другими федеральными законами;

- получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами;

- основываться на ПД Работника, полученных исключительно в результате их автоматизированной обработки или электронного получения при принятии решений, затрагивающих интересы Работника.

7.6. Банк, Работники и их представители совместно вырабатывают меры защиты ПД Работников. В частности, Работники не должны отказываться от своих прав на сохранение и защиту тайны. При этом защита ПД Работника от неправомерного их использования или утраты обеспечивается Банком за счет его средств в порядке, установленном Трудовым кодексом и иными федеральными законами.

7.7. При передаче ПД Работника Банк обязуется соблюдать следующие требования:

- не сообщать ПД Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Работника, а также в других случаях, предусмотренных Трудовым кодексом или иными федеральными законами;

- не сообщать ПД Работника в коммерческих целях без его письменного согласия;

- предупреждать лиц, получающих ПД Работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПД Работника, обязаны соблюдать режим секретности (конфиденциальности), за исключением обмена ПД работников в порядке, установленном Трудовым кодексом и иными федеральными законами;

- осуществлять передачу ПД Работника в пределах одной организации в соответствии с локальным нормативным актом, с которым Работник должен быть ознакомлен под роспись;

- разрешать доступ к ПД Работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПД, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья Работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;

- передавать ПД Работника представителям Работников в порядке, установленном Трудовым кодексом и иными федеральными законами, и ограничивать эту информацию только теми ПД Работника, которые необходимы для выполнения указанными представителями их функций.

7.8. В целях обеспечения защиты ПД, хранящихся в Банке, Работники имеют право:

• получать полную информацию о своих ПД и их обработке (в том числе автоматизированной);

• на свободный бесплатный доступ к своим ПД, включая право получать копии любой записи, содержащей ПД Работника, за исключением случаев, предусмотренных федеральным законом;

• определение своих представителей для защиты своих ПД;

доступ к медицинской документации, отражающей состояние их здоровья (при условии наличия таковой у Банка в связи с необходимостью соблюдения требований законодательства), с помощью медицинского работника по их выбору;

• требовать исключения или исправления неверных или неполных ПД, а также данных, обработанных с нарушением федерального закона. Работник при отказе Банка исключить или исправить ПД Работника имеет право заявлять в письменной форме Банку о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера Работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

• требовать от Банка уведомления всех лиц, которым ранее были сообщены неверные или неполные ПД Работника, обо всех произведённых в них изменениях или исключениях из них;

• обжаловать в суд любые неправомерные действия или бездействие Банка при обработке и защите ПД.

8. ПРЕКРАЩЕНИЕ ОБРАБОТКИ И УНИЧТОЖЕНИЕ ПД

8.1. Обрабатываемые ПД подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

8.2. В случае выявления неправомерной обработки ПД при обращении Субъекта ПД или его представителя либо по запросу Субъекта ПД или его представителя либо Роскомнадзора Банк обязан осуществить блокирование неправомерно обрабатываемых ПД или обеспечить их блокирование (если обработка ПД осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных ПД при обращении Субъекта ПД или его представителя либо по их запросу или по запросу Роскомнадзора Банк обязан осуществить блокирование ПД, относящихся к этому Субъекту ПД, или обеспечить их блокирование (если обработка ПД осуществляется другим лицом, действующим по поручению Банка) с момента такого обращения или получения указанного запроса на период

проверки, если блокирование ПД не нарушает права и законные интересы Субъекта ПД или третьих лиц.

8.3. В случае подтверждения факта неточности ПД Банк на основании сведений, представленных Субъектом ПД или его представителем либо Роскомнадзором, или иных необходимых документов обязан уточнить ПД либо обеспечить их уточнение (если обработка ПД осуществляется другим лицом, действующим по поручению Банка) в течение 7 рабочих дней со дня представления таких сведений и снять блокирование ПД.

8.4. В случае выявления неправомерной обработки ПД, осуществляемой Банком или лицом, действующим по поручению Банка, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную Обработку ПД или обеспечить ее прекращение лицом, действующим по поручению Банка. В случае, если обеспечить правомерность Обработки ПД невозможно, Банк в срок, не превышающий 10 рабочих дней с даты выявления неправомерности, обязан уничтожить такие ПД или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПД Банк (Служба Комплаенс-контроля) обязан уведомить Субъекта ПД или его представителя, а в случае, если обращение Субъекта ПД или его представителя либо запрос Роскомнадзора были направлены Роскомнадзором, также указанный орган.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПД, повлекшей нарушение прав Субъектов ПД, Банк обязан с момента выявления такого инцидента им, Роскомнадзором или иным заинтересованным лицом уведомить Роскомнадзор в порядке, установленном Федеральным законом.

8.5. В случае достижения цели обработки ПД Банк обязан прекратить Обработку ПД или обеспечить ее прекращение (если она осуществляется другим лицом, действующим по поручению Банка) и уничтожить ПД или обеспечить их уничтожение (если она осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий 30 дней с даты достижения цели обработки ПД, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПД, иным соглашением между Банком и Субъектом ПД либо если Банк не вправе осуществлять обработку ПД без согласия Субъекта ПД на основаниях, предусмотренных Федеральным законом или другими федеральными законами.

8.6. В случае отзыва Субъектом ПД согласия на обработку его ПД Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПД осуществляется другим лицом, действующим по поручению Банка) и в случае, если сохранение ПД более не требуется для целей обработки ПД, уничтожить персональные данные или обеспечить их уничтожение (если обработка ПД осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий 30 дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПД, иным соглашением между Банком и Субъектом ПД либо если Банк не вправе осуществлять обработку ПД без согласия Субъекта ПД на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

В случае обращения Субъекта ПД в Банк с требованием о прекращении обработки ПД Банк обязан в срок, не превышающий 10 рабочих дней с даты получения соответствующего требования, прекратить обработку ПД или обеспечить прекращение такой обработки (если такая обработка осуществляется иным лицом по поручению Банка), за исключением случаев, когда согласно Федеральному закону обработка ПД может производиться без согласия Субъекта ПД. Указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Банком в адрес Субъекта ПД мотивированного уведомления с указанием причин продления срока рассмотрения обращения Субъекта ПД.

8.7. В случае невозможности уничтожения ПД в течение указанных выше сроков, Банк осуществляет блокирование таких ПД или обеспечивает их блокирование (если обработка ПД осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение ПД в срок не более чем 6 месяцев, если иной срок не установлен федеральными законами.

8.8. В случаях, предусмотренных п.8.1 – 8.7 (за исключением случаев уничтожения ПД сотрудников (работников), их родственников, кандидатов на вакантные должности, бывших сотрудников, порядок уничтожения которых установлен п.8.9) Банк организует заседание Комиссии,

формируемой согласно п.10.2, которая рассматривает основания для уничтожения (в случае 8.7 также рассматривает обстоятельства, делающие уничтожение невозможным), составляет акт об уничтожении ПД/блокировке ПД (по форме Приложения 1) и принимает решение об уничтожении (способ уничтожения зависит от вида материального носителя ПД и требований законодательства), блокировании или разблокировании соответственно.

Уничтожение ПД и/или носителей ПД должно происходить в присутствии не менее двух членов комиссии.

8.9. В связи с тем, что ПД сотрудников (работников), их родственников, кандидатов на вакантные должности, бывших сотрудников это категория ПД, которая не связана с осуществлением банковской деятельности и доступ к указанным данным имеет очень ограниченный состав лиц, уничтожение указанной категории ПД осуществляется сотрудниками Кадрового подразделения.

По истечении срока хранения соответствующих документов, установленного законодательством, достижении цели обработки ПД. а также в иных установленных Федеральным законом случаях, когда соответствующие документы, содержащие ПД сотрудников, подлежат уничтожению, Кадровое подразделение составляет акт об уничтожении, которые подписывается двумя сотрудниками Кадрового подразделения.

На уничтожение ПД нескольких соискателей может быть составлен один акт при условии соблюдения следующих требований: 1) в акте не отражаются ПД кандидатов, только номера материальных носителей; 2) одновременное уничтожение не повлечет нарушения требований к обработке ПД и сроков хранения ПД ни по одному из кандидатов.

9. ОБРАЩЕНИЯ СУБЪЕКТОВ ПД, РОСКОМНАДЗОРА

9.1. В случае обращения Субъекта ПД, его Представителя, Роскомнадзора с запросом относительно обработки ПД, Банк фиксирует обращение в журнале регистрации входящей корреспонденции и передает запрос на рассмотрение в Службу комплаенс-контроля.

Служба комплаенс-контроля обязана:

1) зафиксировать обращение в Журнале учета обращений по вопросам обработки ПД (Приложение 2) и обеспечить предоставление своевременного и достоверного ответа в срок, соответствующий требованиям законодательства (в течение 10 рабочих дней с даты получения запроса Субъекта ПД или его законного представителя);

2) сообщить Субъекту ПД или его законному представителю информацию о наличии ПД, относящихся к соответствующему Субъекту ПД, а также предоставить возможность ознакомления с ними при обращении Субъекта ПД или его законного представителя либо в течение 10 рабочих дней с даты получения запроса (указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления в адрес Субъекта ПД подготовленного Службой комплаенс-контроля мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации).

9.2. Банк обязан безвозмездно предоставлять Субъекту ПД или его законному представителю возможность ознакомления с ПД, относящимися к соответствующему субъекту ПД, а также в срок не позднее 7 рабочих дней с даты предоставления Субъектом ПД или его представителем сведений, подтверждающих, что ПД являются неполными, неточными или неактуальными вносить в них необходимые изменения. В не позднее 7 рабочих дней с даты представления Субъектом ПД или его представителем сведений, подтверждающих, что такие ПД являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Банк обязан уничтожить такие ПД. О внесенных изменениях и предпринятых мерах Банк обязан уведомлять Субъекта ПД или его законного представителя и третьих лиц, которым ПД этого субъекта были переданы.

9.3. В случае отказа в предоставлении Субъекту ПД или его законному представителю при обращении либо при получении запроса субъекта ПД или его законного представителя информации о наличии ПД о соответствующем субъекте ПД, а также таких ПД Банк обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение ч. 8 ст.14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 10 рабочих дней со дня обращения Субъекта ПД или его законного представителя либо с даты

получения запроса Субъекта ПД или его законного представителя (указанный срок может быть продлен, но не более чем на 5 рабочих дней в случае направления Оператором в адрес Субъекта ПД мотивированного уведомления с указанием причин продления срока рассмотрения запроса).

9.4. В случае обращения Роскомнадзора или иных надзорных органов, осуществляющих контроль и надзор в области персональных данных с любым запросом относительно ПД, порядка их хранения, обработки, уничтожения, проверки соответствия стандартам в области защиты ПД, Банк фиксирует обращение в журнале регистрации входящей корреспонденции и передает запрос на рассмотрение в Службу комплаенс-контроля. Служба комплаенс-контроля в срок, установленный законодательством (для обращений Роскомнадзора - в течение 10 рабочих дней с даты получения такого запроса с возможностью продления не более чем на 5 рабочих дней по мотивированному уведомлению Банка, направленному Роскомнадзору) организует подготовку и отправку ответа, привлекая иные подразделения Банка, к компетенции которых может относиться тематика запроса. Руководство Банка (Президент или Вице-президент) в обязательном порядке информируются о факте и условиях запроса.

10. КОНТРОЛЬ ПРАВИЛЬНОСТИ ОБРАБОТКИ ПД

10.1. С целью обеспечения надлежащего уровня контроля над соблюдением положений действующего законодательства, стандартов Банка России, настоящего Положения, а также иных внутренних документов Банка, в случае, если проверка Службы внутреннего аудита, Службы комплаенс-контроля или иного подразделения Банка выявила факт несоблюдения, то подлежит созыву Комиссия по персональным данным (далее – Комиссия) для рассмотрения всех обстоятельств данного факта. Комиссия также может быть созвана для рассмотрения любого иного вопроса, касающегося обработки персональных данных.

10.2. Комиссия формируется приказом Президента Банка. Состав комиссии может быть пересмотрен в любое время. В случае увольнения или длительного отсутствия одного или нескольких Работников, входящих в состав Комиссии, ее состав пересматривается на следующем запланированном заседании Комиссии, на котором члены Комиссии одобряют кандидатов на включение в состав, после чего проект Приказа представляется на подписание Президенту Банка.

Комиссия осуществляет свою деятельность на нерегулярной основе и может быть созвана для рассмотрения любого из вопросов, относящихся к ПД.

10.3. По результатам работы Комиссии составляется протокол заседания, фиксирующий рассмотренные вопросы и принятые решения, в случае, если предметом рассмотрения комиссии было нарушение правил обработки ПД, то протокол должен содержать описание выявленных нарушений и меры по их устранению и/или предотвращению.

11. ИСПДН

11.1. При обработке ПД с использованием информационных (автоматизированных) систем Банк руководствуется критериями отнесения данных систем к ИСПДН. Такие критерии предлагаются сотрудниками, отвечающими за информационную безопасность, согласуются с членами Комиссии и утверждаются Приказом Президента Банка.

11.2. Отнесение той или иной системы к ИСПДН и определение её типа осуществляется Комиссией на основании критериев, упомянутых в п.11.1 выше. Результаты классификации подлежат фиксации в протоколе заседания.

Приложение 1

Утверждаю

_____

(Ф.И.О должностного лица)

*Место составления*_____
Дата составления «___» _____20__ г.

Акт об уничтожении/блокировании персональных данных

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

установила, что в соответствии с требованиями законодательства и внутренних документов Банка следующие персональные данные (ПД), содержащиеся на материальных носителях, перечисленных ниже, подлежат

☐уничтожению/☐ блокированию ☐ разблокированию в связи с (указать причину)
_____:

№ п/п	Дата учета	Тип носителя	Регистрационный номер носителя ПД	Примечание

Всего подлежит _____ ПД с _____ материальных носителей путем _____.

☐ материальные носители ПД сверены с Актом;

☐ ПД уничтожены вместе с материальным носителем;

☐ ПД уничтожены, уничтожение (стирание) с материального носителя проверено;

☐ ПД в электронном виде, дублирующие данные на материальных носителях, хранящиеся в вычислительных системах и базах данных, удалены;

☐ уничтоженные носители из Журнала учета списаны;

☐ ПД блокированы «___»_____20__ на срок по «____»_____ 20___.

☐ ПД разблокированы «___»_____20__

Особые отметки _____

Председатель комиссии:_____ /
/

Члены комиссии : _____ /
/

_____ /
/

1. В случае уничтожения ПД или носителей ПД разного типа, а также ПД нескольких субъектов ПД может быть составлен один Акт, в котором все носители подлежат перечислению списочным порядком.
2. Все листы акта, а также все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.

Приложение 2

Журнал учета обращений по вопросам обработки персональных данных
Акционерного общества «Сумитомо Мицуи Рус Банк»
(наименование организации БС РФ)

Журнал начат «01» декабря 2009 г.
Должность
_____ / ФИО должностного лица /

Журнал завершен «____» _____ 20___ г.
Должность
_____ / ФИО должностного лица /

№	Сведения о запрашивающем лице	Краткое содержание обращения и цель запроса	Первичное/ Повторное	Отметка о предоставлении информации или отказе в ее предоставлении	Дата передачи/ отказа в предоставлении информации	Подпись ответственного лица	Примечание
1	2	3	4	5	6	7	8

Приложение 3

Журнал учета машинных носителей персональных данных
Акционерного общества «Сумитомо Мицуи Рус Банк»

Раздел I. Учет съемных машинных носителей персональных данных

N п/п	Вид машинного носителя	Номер машинного носителя	Дата постановки на учет машинного носителя	Ф.И.О., должность работника, получившего машинный носитель в пользование	Дата и подпись работника в получении машинного носителя	Дата возврата и/или дата передачи машинного носителя/ основание передачи	Отметка об уничтожении машинного носителя (номер и дата акта)
1	2	3	4	5	6	7	8

Раздел II. Учет несъемных машинных носителей персональных данных

N п/п	Наименование ИС, вид машинного носителя, его местонахождение	Номер машинного носителя/номер техпаспорта на ИС	Дата постановки на учет	Дата возврата или окончания эксплуатации машинного носителя	Отметка об уничтожении машинного носителя (номер и дата акта)
1	2	3	4	7	8