Утверждено
Приказом Председателя
Правления
№ 72
от «_01_» ___04__ 2021 г.

Положение

об обработке персональных данных

в АО КБ «РУСНАРБАНК»

2021

Обозначения и сокращения

АБС — автоматизированная банковская система;
БС — банковская система;
ЖЦ — жизненный цикл;
ИБ — информационная безопасность;
ИСПДн — информационная система персональных данных;
НСД — несанкционированный доступ;
НРД — нерегламентированные действия в рамках предоставленных полномочий;
ПДн – персональные данные;
СКЗИ — средство криптографической защиты информации;
СМИБ — система менеджмента информационной безопасности;
СИБ — система информационной безопасности;
СОИБ — система обеспечения информационной безопасности;

1. Общие положения

1.1. Настоящее «Положение об обработке персональных данных в АО КБ «РУСНАРБАНК» (далее – Положение) устанавливает порядок обработки персональных данных в Банке в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ № 152-ФЗ), рекомендациями Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014», нормами Корпоративной и Частных политик информационной безопасности АО КБ «РУСНАРБАНК».

1.2. Задачей Банка является обеспечение в соответствии с законодательством Российской Федерации защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну работников Банка, клиентов и иных субъектов ПДн.

1.3. В соответствии с нормами ст. 18.1 ФЗ № 152-ФЗ для обеспечения неограниченного доступа к документам Банка, определяющим его политику в отношении обработки ПДн и к сведениям о реализуемых требованиях к защите ПДн, настоящее Положение наряду с «Частной политикой информационной безопасности при обработке персональных данных в АО КБ «РУСНАРБАНК» подлежат размещению на доске объявлений в операционных зонах внутренних структурных подразделениях Банка и на сайте Банка www.rusnarbank.ru.

2. Принципы обработки ПДн

2.1. Банк обрабатывает ПДн в соответствии со следующими принципами:

- обработка ПДн в Банке ограничивается достижением заранее определённых и законных целей,
- не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой,
- обработке подлежат только ПДн, которые отвечают целям их обработки,
- содержание и объём обрабатываемых ПДн должны соответствовать заявленным целям обработки,
- при обработке ПДн должно быть обеспечена их точность, достаточность и актуальность по отношению к целям обработки ПДн,
- хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн,

- обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки.

2.2. В Банке не обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, характеризующие физиологические особенности человека и на основе которых, можно установить его личность, за исключением случаев, предусмотренных ТК РФ и другими федеральными законами.

3. Порядок обработки ПДн

3.1. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу. Перечень ПДн, обрабатываемых в Банке, а также цели их обработки, приведены в Приложении № 1 к настоящему Положению.

3.2. Банк осуществляет обработку ПДн:

- обрабатываемых в соответствии с трудовым законодательством,
- полученных в связи с заключением договора, стороной которого, либо выгодоприобретателем или поручителем, по которому, является субъект ПДн, при этом ПДн не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются Банком исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн,
- разрешенных субъектом ПДн для распространения при условии соблюдения Банком запретов и условий, предусмотренных статьей 10.1 ФЗ № 152-ФЗ,
- включающих в себя только фамилии, имена и отчества субъектов ПДн,
- необходимых в целях однократного пропуска субъекта ПДн на территорию Банка,
- включенных в информационные системы ПДн, имеющие в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка.

3.3. Банк не осуществляет трансграничную передачу ПДн.

3.4. С учетом особенностей обработки ПДн в соответствии с нормами статьи 22 ФЗ № 152-ФЗ Банк вправе осуществлять обработку ПДн без уведомления уполномоченного органа по защите прав субъектов ПДн.

3.5. Обработка ПДн осуществляется в соответствии с нормативно-правовыми актами Российской Федерации из заключаемых Банком трудовых договоров, гражданско-правовых сделок, в результате совершения Банком операций и сделок в процессе своей обычной хозяйственной деятельности.

3.6. Без согласия субъектов осуществляется обработка общедоступных ПДн или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка ПДн для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации.

3.7. В случае достижения целей обработки ПДн, Банк обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн в сроки, предусмотренные законодательством или соглашением с субъектом ПДн.

3.8. Обработка ПДн в Банке осуществляется в смешанном полуавтоматическом режиме, с использованием бумажных носителей и программных средств.

3.9. Право на обработку ПДн предоставляется работникам Банка в соответствии с выполняемыми ими своих должностных обязанностей и в соответствии с нормами «Положение о коммерческой тайне АО КБ «РУСНАРБАНК».

3.10. При отнесении АБС к информационным системам ПДн / ИСПДн, Банк использует следующий подход:

В перечень ИСПДн Банк включает АБС, целью создания и использования которых, является обработка ПДн.

3.11. Правила обработки и использования ПДн, включая сроки хранения оригиналов документов или копий документов на записываемых оптических носителях, предназначенных для архивного хранения, устанавливаются приказами, регламентами и инструкциями Банка, в том числе номенклатурой дел Банка.

3.12. ПДн уничтожаются по достижении целей их обработки в течение трёх рабочих дней, а также по иным основаниям, предусмотренным ФЗ № 152-ФЗ.

Решение об уничтожении принимается экспертной комиссией, созданной в соответствии с Положением об экспертной комиссии в Банке. Уничтожение производится в присутствии членов комиссии, о чем составляется акт (форма Акта уничтожения носителей ПДн приведена в Приложении № 5 к настоящему Положению). Об уничтожении ПДн, ответственный работник архива Банка уведомляет субъектов персональных данных.

4. Меры, принимаемые Банком для защиты ПДн

4.1. При обработке ПДн Банк принимает необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении ПДн.

4.2. Обеспечение безопасности ПДн в Банке может достигаться, посредством:

1) определения угроз безопасности ПДн при их обработке в ИСПДн (угроз информационной безопасности);

2) применения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн, исполнение которых, обеспечивает установленные Правительством Российской Федерации уровни защищённости ПДн;

3) применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн;

5) учёта машинных носителей с ПДн;

6) обнаружения фактов несанкционированного доступа к ПДн и принятием мер;

7) восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установления правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечения регистрации и учёта всех действий, совершаемых с ПДн в ИСПДн;

9) контроля за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищённости ИСПДн.

4.3. В целях обеспечения безопасности ПДн, обрабатываемых без использования средств автоматизации, в отношении каждой категории ПДн Банком определяются их места хранения (материальные носители) и устанавливается перечень лиц, осуществляющих обработку ПДн, либо имеющих к ним доступ. Банком обеспечивается раздельное хранение ПДн (материальные носители), обработка которых, осуществляется в различных целях.

При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ, в частности:

- документы и иные носители, содержащие ПДн, хранятся в запираемых шкафах, металлических ящиках, сейфах с установленными на них опечатывающих устройств, а также в запираемых помещениях, к которым ограничен допуск работникам;
- все помещения Банка находятся на контролируемой территории под круглосуточной охраной, входы в помещения находятся под видеонаблюдением, а в нерабочее время ставятся на сигнализацию.

- в Банке установлен перечень лиц, ответственных за безопасность ПДн при работе в ИСПДн.

4.4. В целях исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при обработке в информационных системах, Банк использует 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 ПДн), а также использует в информационной системе современные информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

4.5. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Классификация ИСПДн осуществляется Банком в порядке, установленном законодательством Российской Федерации.

4.6. Обмен ПДн при их обработке в информационных системах осуществляется по каналам связи, защита которых, обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с ПДн, организация режима обеспечения безопасности в этих помещениях, должны обеспечивать сохранность носителей ПДн и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.7. С целью повышения безопасности ПДн, обрабатываемых в ИСПДн, Банк может проводить процедуры обезличивания, т.е. осуществлять действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн.

Решение о проведении обезличивания ПДн и проведения, в случае необходимости, повторной классификации ИСПДн принимается Председателем Правления на основании Заключения о возможности обезличивания ПДн, предоставленной работником ответственным за обработку ПДн.

5. Права, обязанности и ответственность субъекта ПДн и Банка при обработке ПДн

5.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

1) подтверждение факта обработки ПДн Банком;

2) правовые основания и цели обработки ПДн;

3) цели и применяемые Банком способы обработки ПДн;

4) наименование и место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн, или которым могут быть раскрыты ПДн на основании договора с Банком или на основании ФЗ № 152-ФЗ;

5) обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен ФЗ № 152-ФЗ;

6) сроки обработки ПДн, в том числе сроки их хранения;

7) информацию об осуществлённой или о предполагаемой трансграничной передаче данных;

8) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные ФЗ № 152-ФЗ или другими федеральными законами.

5.2. Право субъекта ПДн на доступ к его данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

3) обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

5) обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

5.3. Субъект ПДн вправе требовать от Банка уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

5.4. Банк отвечает на обращения субъектов ПДн или их законных представителей по вопросам обработки ПДн с учётом следующего:

5.4.1. Сведения, указанные в п. 5.1., должны быть предоставлены субъекту ПДн Банком в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

5.4.2. Сведения, указанные в п. 5.1. предоставляются субъекту ПДн или его законному представителю при обращении, либо при получении запроса субъекта ПДн или его законного представителя.

Запрос должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с Банком (номер договора, дата заключения договора и иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком, подпись субъекта ПДн или его представителя.

Обращения субъектов ПДн фиксируются Банком в Журнале учета обращений граждан (субъектов ПДн) по вопросам обработки ПДн.

5.4.3. В случае, если сведения, указанные в п. 5.1., а также обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно в Банк в целях получения сведений, указанных в п. 5.1., и ознакомления с такими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен ФЗ № 152-ФЗ, принятым в соответствии с ним нормативным правовым актом или договором с Банком, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

5.4.4. Банк обязан безвозмездно предоставить субъекту ПДн или его законному представителю возможность ознакомления с ПДн, относящимися к соответствующему субъекту ПДн, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие ПДн по предоставлении субъектом ПДн или его законным представителем сведений, подтверждающих, что ПДн, которые относятся к соответствующему субъекту и обработку которых осуществляет Банк, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Банк обязан уведомить субъекта ПДн или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

5.5. Банк отвечает на запросы уполномоченного органа по защите прав субъектов ПДн или иных надзорных органов, осуществляющих контроль и надзор в области ПДн, с учётом следующего:

Банк обязан сообщить в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса. Иным надзорным органам Банк предоставляет информацию в случаях, предусмотренных законодательством РФ, при предоставлении в Банк мотивированного запроса.

5.6. В случае выявления неправомерных действий с ПДн Банк в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Банк в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с ПДн, обязан уничтожить ПДн. Об устранении допущенных нарушений или об уничтожении ПДн Банк обязан уведомить субъекта ПДн или его законного представителя.

5.7. В случае отзыва субъектом ПДн согласия на обработку своих ПДн Банк обязан прекратить обработку ПДн и уничтожить ПДн в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено законодательством Российской Федерации, договором или соглашением между Банком и субъектом ПДн. Об уничтожении ПДн Банк обязан уведомить субъекта ПДн.

5.8. Банк не вправе без письменного согласия субъекта ПДн передавать обрабатываемые ПДн третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации.

5.8. Банк, а также должностные лица, виновные в нарушении требований Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании ПДн возлагается на лицо, ответственное за обеспечение безопасности ПДн в Банке и конкретных должностных лиц Банка, обрабатывающих ПДн.

Приложение № 1
к «Положению
об обработке персональных данных
в АО КБ «РУСНАРБАНК»

**Перечень персональных данных,
обрабатываемых в АО КБ «РУСНАРБАНК»**

1. Общие положения

Перечень персональных данных, подлежащих обработке в АО КБ «РУСНАРБАНК» (далее Банк), разработан в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Сведения, составляющие персональные данные

В Банке сведениями, составляющими ПДн, является любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных), в том числе:

- Фамилия, имя, отчество, дата и место рождения.
- Паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ) и гражданство.
- Адрес места жительства (по паспорту и фактический) и дата регистрации по месту жительства или по месту пребывания.
- Номера телефонов.
- Конкретизированные сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки, о повышении квалификации и переподготовке, а именно: серия, номер, дата выдачи диплома, свидетельства, аттестата или другого документа об окончании образовательного учреждения, в том числе наименование и местоположение образовательного учреждения.
- Сведения о трудовой деятельности (данные о трудовой занятости на текущее время с полным указанием должности, подразделения, организации и её наименования, ИНН, адреса и телефонов, а также реквизитов других организаций с полным наименование занимаемых ранее в них должностей и времени работы в этих организациях).
- Сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в неё) и записях в ней.
- Содержание и реквизиты трудового договора с работником Банка или гражданско-правового договора с гражданином.
- Сведения о заработной плате (номера счетов для расчёта с работниками Банка, данные зарплатных договоров с клиентами, в том числе номера их спецкартсчетов).
- Сведения о воинском учёте военнообязанных лиц и лиц, подлежащих призыву на военную службу (серия, номер, дата выдачи, наименование органа, выдавшего военный билет) из числа работников Банка.
- Конкретизированные сведения о семейном положении, а именно: данные свидетельства о заключении брака, фамилия, имя, отчество супруга(и), паспортные данные супруга(и), данные брачного контракта, данные справки по форме 2НДФЛ супруга(и), данные документов по долговым обязательствам, степень родства, фамилии, имена, отчества и даты рождения других членов семьи, иждивенцев.
- Оценка навыков и личностных качеств.

- Сведения об имуществе (имущественном положении):
  - автотранспорт (государственные номера и другие данные из свидетельств о регистрации транспортных средств и из паспортов транспортных средств);
  - недвижимое имущество (полные адреса размещения объектов недвижимости);
  - банковские вклады (данные договоров с клиентами, в том числе номера их счетов, спецкартсчетов);
  - кредиты, банковские счета, денежные средства и ценные бумаги, в том числе в доверительном управлении и на доверительном хранении (данные договоров с клиентами, в том числе номера счетов, номера банковских карт, кодовая информация по банковским картам, коды кредитных историй, адреса приобретаемых объектов недвижимости).
- Сведения о номере и серии страхового свидетельства государственного пенсионного страхования.
- Сведения об идентификационном номере налогоплательщика.
- Сведения из страховых полисов обязательного (добровольного) медицинского страхования (в том числе данные соответствующих карточек медицинского страхования).
- Сведения, указанные в оригиналах и копиях приказов по личному составу Банка и материалах к ним.
- Медицинские заключения установленной формы об отсутствии у гражданина заболевания, препятствующего или ограничивающие выполнению трудовых функций (в соответствии с требованиями Трудового кодекса Российской Федерации и других федеральных законов - в отношении категорий работников Банка, подлежащих медицинским осмотрам).
- Внутрибанковские материалы по расследованию и учёту несчастных случаев на производстве и профессиональным заболеваниям в соответствии с Трудовым кодексом Российской Федерации, другими федеральными законами.
- Сведения о временной нетрудоспособности работников Банка.
- Табельный номер работника Банка.
- Фотоизображение субъекта ПДн (качеством не хуже изображения в паспорте РФ).
- Фотография или видеозапись человека, позволяющие его идентифицировать.
- Биометрические данные.

3. Цели обработки персональных данных

Целью обработки персональных данных является реализация заключаемых Банком договоров с клиентами и контрагентами, осуществление возложенных на Банк законодательством Российской Федерации и Уставом Банка функций.

Разовый проход клиентов и посетителей Банка на территорию Банка и помещения в зоне ограниченного доступа.

А также организация учёта работников Банка для обеспечения соблюдения законов и иных нормативно-правовых актов.

4. Сроки обработки персональных данных

Сроки обработки указанных выше персональных данных определяются:

- в соответствии со сроком действия договора с субъектом персональных данных, утвержденной в Банке номенклатурой дел, сроком исковой давности,

- в соответствии с требованиями части 7 статьи 5 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».