

Утверждено:

Правлением ПАО «ЧЕЛЯБИНВЕСТБАНК»

Протокол № 153 от «19» июля 2017 г.

№ 23 - 018 - П

ПОЛИТИКА
обработки персональных данных
в ПАО «ЧЕЛЯБИНВЕСТБАНК»

версия 1.1.

Челябинск
2017

ОГЛАВЛЕНИЕ

1.	ОБЩИЕ ПОЛОЖЕНИЯ	3
1.1.	Область применения	3
1.2.	Термины и определения	3
1.3.	Сокращения	4
2.	ОСНОВНЫЕ ПОЛОЖЕНИЯ	4
2.1.	Принципы обработки персональных данных	4
2.2.	Цели обработки персональных данных	4
2.3.	Субъекты персональных данных	5
2.4.	Состав персональных данных	5
2.5.	Согласие на обработку персональных данных	6
2.6.	Поручение на обработку персональных данных	6
2.7.	Способы обработки	6
2.8.	Период обработки и хранения персональных данных	7
3.	ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ	7
4.	ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ	8
5.	ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	9

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения

1.1.1. Настоящая Политика определяет систему взглядов на обеспечение безопасности персональных данных в ПАО «ЧЕЛЯБИНВЕСТБАНК» и представляет собой систематизированное изложение целей и задач защиты, основных принципов и способов обеспечения требуемого уровня безопасности информации, организационных и технологических аспектов обеспечения безопасности персональных данных в информационных системах.

1.1.2. Настоящая Политика определяет главные принципы, которыми руководствуется Банк при обработке персональных данных в процессе осуществления своей деятельности.

1.1.3. Настоящая Политика разработана в соответствии с положениями действующих нормативно-правовых актов Российской Федерации, в том числе:

- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.1.4. Целью настоящей Политики является формирование и проведение единой политики в области обеспечения безопасности персональных данных.

1.1.5. Действие настоящей Политики распространяется на все процессы Банка, связанные с обработкой персональных данных, и обязательна для применения всеми работниками Банка.

1.1.6. Внутренние документы Банка, затрагивающие вопросы, рассматриваемые в настоящей Политике, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

1.1.7. На основании приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Банк включен в реестр операторов, осуществляющих обработку персональных данных.

1.1.8. Настоящая Политика размещена в открытом неограниченном доступе на Интернет-сайте Банка (<https://chelinvest.ru/about/charter/>).

1.1.9. Пересмотр и обновление настоящей Политики осуществляется в связи с изменениями законодательства Российской Федерации в области персональных данных, по результатам анализа актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, а также по результатам других контрольных мероприятий.

1.2. Термины и определения

Автоматизированная Обработка Персональных данных – Обработка персональных данных с помощью средств вычислительной техники;

Блокирование персональных данных – временное прекращение Обработки персональных данных (за исключением случаев, если Обработка необходима для уточнения Персональных данных);

Информационная система Персональных данных – совокупность содержащихся в базах данных Персональных данных и обеспечивающих их Обработку информационных технологий и технических средств;

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 – любое действие (операция) или совокупность действий (операций), совершаемых с Персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (Распространение, Предоставление, доступ), Обезличивание, Блокирование, удаление, Уничтожение персональных данных;

Ответственный за организацию обработки персональных данных – должностное лицо, которое назначается Приказом Председателя Правления, организующее принятие правовых, организационных и технических мер в целях обеспечения надлежащего выполнения функций по

организации Обработки персональных данных в Банке в соответствии с положениями законодательства Российской Федерации в области Персональных данных;

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту Персональных данных);

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

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

Субъект персональных данных – физическое лицо, прямо или косвенно определенное или определяемое на основании относящихся к нему Персональных данных;

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

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

1.3. Сокращения

Банк – ПАО «ЧЕЛЯБИНВЕСТБАНК»;

ПД – Персональные данные;

ИСПД - Информационная система персональных данных;

Политика - Политика обработки персональных данных в ПАО «ЧЕЛЯБИНВЕСТБАНК» – настоящий документ

ФЗ «О персональных данных» - Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1. Принципы обработки персональных данных

2.1.1. Обработка ПД в Банке осуществляется на основании следующих принципов:

- законности и справедливости целей и способов обработки ПД;
- соответствия целей обработки ПД законным целям, заранее определенным и заявленным при сборе ПД, а также полномочиям Банка;
- соответствия объема и содержания обрабатываемых ПД, способов обработки ПД целям обработки ПД;
- точности ПД, их достаточности для целей обработки, недопустимости обработки ПД, избыточных по отношению к целям, заявленным при сборе ПД;
- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих ПД;
- хранения ПД в форме, позволяющей определить субъекта ПД, не дольше, чем этого требуют цели обработки ПД, или устанавливающий срок хранения федеральный закон, договор, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД;
- уничтожения или обезличивание ПД по достижении целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения ПД, установленного федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД;
- обеспечения конфиденциальности и безопасности обрабатываемых персональных данных.

2.2. Цели обработки персональных данных

2.2.1. Целями обработки ПД являются:

- выполнение работ, услуг, функций, полномочий и обязанностей, определенных Уставом, лицензиями и внутренними документами Банка, договорных обязательств Банка перед клиентами, предоставления возможности работникам контрагентов Банка выполнения обязанностей, предусмотренных договорами между Банком и его контрагентами;
- осуществление возложенных на Банк законодательством Российской Федерации функций (в том числе по передаче сведений третьим лицам) в соответствии с законодательством РФ об исполнительном производстве, Налоговым кодексом Российской Федерации, федеральными законами, в том числе: «Об организации предоставления государственных и муниципальных услуг», «О банках и банковской деятельности», «О противодействии легализации (отмыванию) доходов, полученных преступным путем,

и финансированию терроризма», «О несостоятельности (банкротстве)», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О кредитных историях», «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях»;

- организация учета работников Банка для обеспечения соблюдения законов и иных нормативных правовых актов, содействие субъектам ПД в трудоустройстве, обучении, продвижении по службе, очередности предоставления отпусков, расчета размера заработной платы, использования различных форм страхования, обеспечения пропускного режима Банка, обеспечения личной безопасности работников и сохранности имущества, контроля количества и качества выполняемой работы, пользовании различного вида льготами в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, федеральными законами, заключенными с субъектами ПД договорами, а также Уставом и внутренними документами Банка.

2.3. Субъекты персональных данных

2.3.1. Субъектами ПД в Банке являются:

- клиенты Банка - физические лица, в том числе потенциальные;
- представители (работники) клиентов и контрагентов Банка, в том числе представители потенциальных клиентов и контрагентов;
- физические лица, заключившие или планирующие заключить с Банком гражданско-правовой договор, в том числе, физические лица – представители юридических лиц, заключивших или планирующих заключить с Банком гражданско-правовой договор;
- соискатели вакантных должностей в Банке;
- действующие и уволенные работники Банка, а также члены их семей;
- аффилированные лица и инсайдеры Банка;
- иные физические лица, выразившие согласие на обработку Банком их персональных данных, или физические лица, обработка ПД которых необходима Банку для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных на Банк функций, полномочий и обязанностей.

2.4. Состав персональных данных

2.4.1. В процессе своей деятельности Банк осуществляет обработку следующих персональных данных:

- фамилия, имя, отчество (в том числе прежние);
- пол;
- дата и место рождения;
- паспортные данные, данные других документов, удостоверяющих личность (серия, номер, дата выдачи, код подразделения, наименование органа, выдавшего документ);
- гражданство;
- статус резидента;
- семейное положение;
- места жительства (адрес регистрации, адрес проживания);
- электронный адрес (e-mail);
- номера контактных телефонов;
- место работы и должность;
- идентификационный номер налогоплательщика;
- номер пенсионного удостоверения;
- информация о счетах, включая информацию об остатках и операциях по ним;
- иная информация, необходимая Банку для осуществления услуг, согласно заключенному договору.

2.4.2. Для лиц, изъявивших желание воспользоваться кредитными продуктами, Банк дополнительно осуществляет обработку следующих персональных данных:

- образование и профессия;
- уровень платежеспособности (уровень дохода);
- данные, содержащиеся в трудовой книжке;
- контактная информация о текущем и предыдущих местах работы;
- информация о составе семьи;
- информация о финансовом состоянии;
- информация об имущественных правах;

- информация об обязательствах, в том числе алиментных.

2.4.3. Для лиц, являющихся работниками Банка или проходящих процедуры оформления на работу с целью заключения трудового договора, Банк дополнительно осуществляет обработку следующих персональных данных:

- образование и профессия;
- сведения о воинском учете;
- данные, содержащиеся в трудовой книжке;
- контактная информация о текущем и предыдущих местах работы;
- фотография;
- информация о составе семьи;
- фамилии, имена и отчества, даты и места рождения родственников;
- знание иностранных языков (каких и степень знания);
- другая информация, представленная соискателем в резюме (анкете).

2.4.4. Банк не осуществляет обработку специальных категорий ПД, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни, судимости физических лиц, если иное не установлено законодательством Российской Федерации.

2.5. **Согласие на обработку персональных данных**

2.5.1. Получение и обработка ПД осуществляется Банком с письменного согласия субъекта ПД.

2.5.2. Письменное согласие субъекта ПД должно включать:

- фамилию, имя, отчество, адрес субъекта ПД/представителя субъекта ПД, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование и адрес Банка;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПД по поручению Банка, если обработка будет поручена такому лицу;
- цель обработки ПД;
- перечень ПД, на обработку которых дается согласие субъекта ПД;
- перечень действий с ПД, на совершение которых дается согласие, общее описание используемых Банком способов обработки ПД;
- срок, в течение которого действует согласие, а также порядок его отзыва;
- подпись субъекта ПД.

2.5.3. Факт подтверждения согласия путем установки соответствующих флагов/переключателей/нажатия кнопок на экранных веб-формах, подтверждающих согласие субъекта с условиями обработки ПД при заполнении анкет на официальном сайте Банка в целях получения услуг, предоставляемых Банком, расценивается Банком как согласие на обработку ПД субъектом, даваемое субъектом в письменном виде с проставлением собственноручной подписи.

2.5.4. Согласие на обработку ПД может быть отозвано субъектом ПД путем направления в Банк письменного заявления в свободной форме. В этом случае Банк обязуется прекратить обработку, а также уничтожить все имеющиеся в Банке ПД в сроки, установленные ФЗ «О персональных данных».

2.5.5. Банк вправе обрабатывать ПД без согласия субъекта ПД (или при отзыве субъектом ПД указанного согласия) при наличии оснований, указанных в ФЗ «О персональных данных».

2.6. **Поручение на обработку персональных данных**

2.6.1. Банк вправе поручить обработку ПД другому лицу с согласия субъекта ПД, если иное не предусмотрено федеральным законом, на основании заключаемого с этой стороной договора (поручения на обработку ПД).

2.6.2. В поручении Банка должны быть определены перечень действий (операций) с ПД, которые будут совершаться лицом, осуществляющим обработку ПД, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность ПД и обеспечивать безопасность ПД при их обработке, а также должны быть указаны требования к защите обрабатываемых ПД в соответствии с ФЗ «О персональных данных».

2.7. **Способы обработки персональных данных**

2.7.1. Обработка ПД Банком осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновление, изменение), извлечения, использования, передачи (распространение, предоставление, доступ), обезличивания, блокирования, удаления, уничтожения.

2.7.2. Банк осуществляет обработку персональных данных следующими способами;

- автоматизированная обработка (производится при помощи средств вычислительной техники);
- неавтоматизированная обработка (производится без участия средств вычислительной техники);
- смешанная обработка (производится как при помощи средств вычислительной техники, так и без них).

2.7.3. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных настоящей Политикой.

2.7.4. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

2.7.5. В случае необходимости осуществления трансграничной передачи персональных данных Банк перед совершением такой передачи обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, а также в отсутствии установленных законодательством запретов или ограничений на передачу персональных данных на территорию данного иностранного государства.

2.7.6. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться Банком в случаях:

- наличия согласия в письменной форме субъекта персональных данных;
- исполнения договора, стороной которого является субъект персональных данных;
- в иных случаях, установленных законодательством РФ.

2.8. Период обработки и хранения персональных данных

2.8.1. Сроки обработки указанных выше ПД определяются в соответствии со сроком действия договора с субъектом ПД, сроком исковой давности, Приказом Министерства культуры Российской Федерации от 25.08.2010 №558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также иными требованиями законодательства Российской Федерации.

2.8.2. Обработка ПД начинается с момента поступления в Банк ПД и прекращается:

- в случае выявления неправомерной обработки ПД Банком или лицом, действующим по поручению Банка. Банк в срок, не превышающий десяти рабочих дней с даты такого выявления, Банк обязан прекратить неправомерную обработку ПД или обеспечить прекращение неправомерной обработки ПД лицом, действующим по поручению Банка. В случае невозможности устранения допущенных нарушений Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с ПД, уничтожает ПД или обеспечивает их уничтожение. Об устранении допущенных нарушений или об уничтожении ПД Банк уведомляет субъекта ПД или его представителя, а в случае, если обращение или запрос были направлены Роскомнадзором – также этот орган;

- в случае достижения цели обработки ПД. Банк незамедлительно прекращает обработку ПД и уничтожает соответствующие ПД в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки ПД;

- в случае отзыва субъектом ПД согласия на обработку своих ПД. Банк прекращает обработку ПД и уничтожает (за исключением ПД, которые хранятся в соответствии с действующим законодательством) ПД в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва. Об уничтожении ПД Банк уведомляет субъекта ПД.

2.8.3. Уничтожение ПД производится в случаях и в сроки, указанные выше, за исключением ПД бухгалтерского и кадрового учета, которые хранятся в соответствии с действующим законодательством Российской Федерации.

3. ПРАВА СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Субъект ПД имеет право на получение информации, касающейся обработки Банком его ПД.

3.2. Субъект ПД вправе требовать от Банка 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.

3.3. Право субъекта ПД на доступ к его ПД может быть ограничено в соответствии с федеральными законами Российской Федерации, в том числе если:

3.3.1. обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

3.3.2. доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

3.4. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только при условии предварительного согласия субъекта ПД.

3.5. Банк принимает и обрабатывает запросы субъектов персональных данных и предоставляет сведения, подтверждающие факты обработки персональных данных, правовые основания, цели, сроки и способы обработки персональных данных, виды обрабатываемых персональных данных, свое наименование и местонахождение.

4. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом «О персональных данных» или другими федеральными законами.

4.2. В Банке принимаются следующие меры по обеспечению выполнения обязанностей, предусмотренных ФЗ «О персональных данных»:

- назначаются лица, ответственные за организацию обработки персональных данных;
- издаются документы, определяющие политику Банка в отношении обработки ПД, локальные акты по вопросам обработки ПД, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

- применяются правовые, организационные и технические меры по обеспечению безопасности ПД;
- осуществляется внутренний контроль и аудит соответствия обработки ПД требованиям законодательства РФ, настоящей Политике, иным локальным актам Банка;

- осуществляется оценка возможного вреда субъектам ПД, причиненного в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Банком мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

- производится ознакомление работников, непосредственно осуществляющих обработку ПД с положениями законодательства РФ о персональных данных, в том числе требованиями к защите ПД, настоящей Политикой и иными локальными актами Банка по вопросам обработки персональных данных и (или) обучение указанных работников;

- обеспечивается обработка ПД граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пункте 5 статьи 18 ФЗ «О персональных данных».

4.3. Обеспечение безопасности ПД достигается:

- определением угроз безопасности ПД при их обработке в ИСПД;
- применением организационных и технических мер по обеспечению безопасности ПД при их обработке в ИСПД, необходимых для выполнения требований к защите ПД, исполнение которых обеспечивает установленные уровни защищенности ПД;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности ПД до ввода в эксплуатацию ИСПД;

- обеспечением учета и сохранности носителей ПД;

- своевременным уничтожением и обезличиванием ПД;

- обнаружением фактов несанкционированного доступа к ПД и принятием мер;

- восстановлением ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установлением правил доступа к ПД, обеспечением регистрации и учета всех действий, совершаемых с ПД в ИСПД;
- контролем за принимаемыми мерами по обеспечению безопасности ПД и уровня защищенности ИСПД.

4.4. Меры по обеспечению безопасности ПД принимаются 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 и направлены на нейтрализацию актуальных угроз безопасности ПД.

4.5. Состав и содержание организационных и технических мер безопасности ПД устанавливается в соответствии с внутренними документами Банка.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

5.1. Контроль исполнения требований настоящей Политики осуществляется Ответственным за организацию обработки персональных данных в Банке.

5.2. В случае изменений законодательных и иных нормативных актов Российской Федерации, а также Устава Банка, настоящий документ, а также изменения к нему, применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Банка.

5.3. Банк имеет право вносить изменения в настоящую Политику. При внесении изменений в заголовке Политики указывается дата утверждения Политики и номер версии (редакции).

5.4. Настоящая Политика вступает в силу с момента утверждения Правлением Банка.