УТВЕРЖДЕНО

Решением Совета директоров

АО «БАНК БЕРЕЙТ»

Протокол № 26/2020 от 23.10.2020 года

**ПОЛИТИКА**

**В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ**

**АО «БАНК БЕРЕЙТ»**

**Ленинградская обл.**

**г.п. Красный Бор**

 **2020**

## Оглавление

[1. Общие положения 3](#_Toc473896886)

[2. Термины и определения 3](#_Toc473896887)

[3. Цели обработки персональных данных 5](#_Toc473896888)

[4. Принципы обработки персональных данных 6](#_Toc473896889)

[5. Условия обработки персональных данных 7](#_Toc473896890)

[6. Права субъекта персональных данных 8](#_Toc473896891)

[7. Обязанности Оператора 9](#_Toc473896892)

[8. Перечень мер, направленных на выполнение обязанностей Оператора 10](#_Toc473896893)

[9. Ответственность Оператора 11](#_Toc473896894)

[10. Раскрытие информации 12](#_Toc473896895)

# ОБЩИЕ ПОЛОЖЕНИЯ

* 1. Политика в отношении обработки персональных данных АО «БАНК БЕРЕЙТ» (далее - Политика) определяет политику Акционерного общества «БАНК БЕРЕЙТ» (далее – Оператор) в отношении обработки и обеспечения информационной безопасности персональных данных.
	2. Настоящая Политика разработана в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», иными Федеральными законами и нормативными актами и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных Оператором.
	3. Целью настоящей Политики является установление основных принципов и подходов к обработке и обеспечению информационной безопасности персональных данных при осуществлении Оператором уставной деятельности.
	4. Действие настоящей Политики распространяется на все внутренние процессы Оператора, связанные с обработкой персональных данных, кроме процессов, организованных во исполнение действующего законодательства Российской Федерации об архивном деле.
	5. Положения настоящей Политики являются обязательными для исполнения всеми работниками Оператора, имеющими доступ к персональным данным.
	6. Настоящая Политика вступает в силу с момента утверждения Советом директоров Оператора и действует вплоть до отмены. Все изменения и дополнения к настоящей Политике утверждаются Советом директоров Оператора в установленном порядке.
	7. Пересмотр настоящей Политики производится Оператором при изменении в законодательных актах Российской Федерации, регулирующих вопросы обработки и защиты персональных данных, а также при появлении специальных нормативных документов в области обработки и защиты персональных данных.

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

***Персональные данные***— любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

***Обработка персональных данных*** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

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

***Предоставление персональных данных*** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

***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.

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

***Информационная система персональных данных*** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

***Трансграничная передача персональных данных*** — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**ВП** – Вредоносная программа

**ИБ** – Информационная безопасность

**ИС** – Информационные системы

**ИСПДн** – Информационные системы персональных данных

**ЛВС** – Локальная вычислительная сеть

**МЭ** – Межсетевой экран

**НСД** – Несанкционированный доступ

**ОС** – Операционная система

**ПДн** – Персональные данные

**ПМВ** – Программно-математические воздействия

**ПО** – Программное обеспечение

**РД** – Руководящий документ

**САЗ** – Средство анализа защищенности

**СВТ** – Средства вычислительной техники

**СЗИ** – Средства защиты информации

**СЗПДн** – Система защиты персональных данных

**СОВ** – Система (средство) обнаружения вторжения

**СИБ** – Служба информационной безопасности Банка

**ФСТЭК** – Федеральная служба по техническому и экспортному контролю России

# ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Целями обработки персональных данных Оператором являются:
* осуществление банковских операций и иной деятельности, предусмотренной Уставом и лицензиями Оператора, нормативными актами Банка России и действующим законодательством Российской Федерации;
* заключение, исполнение и прекращение гражданско-правовых договоров с физическими и юридическими лицами и индивидуальными предпринимателями в случаях, предусмотренных Уставом Оператора и действующим законодательством Российской Федерации;
* организация кадрового учета работников Оператора; ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании различного вида льготами; исполнение требований налогового законодательства Российской Федерации в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога; исполнение требований пенсионного законодательства Российской Федерации при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение; осуществление обязательного и добровольного медицинского страхования работников Оператора; заполнение первичной статистической документации в соответствии с Трудовым кодексом Российской Федерации, Налоговым кодексом Российской Федерации, Федеральными законами Российской Федерации, Уставом и внутренними нормативными документами Оператора.

# ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Политика обработки персональных данных в Банке определяется в соответствии с законодательством Российской Федерации, нормативными актами Банка России, внутренними документами Банка, согласием субъекта персональных данных на обработку его персональных данных.
	2. В целях реализации положений Политики в Банке разрабатываются внутренние нормативные акты и иные документы, регламентирующие вопросы обработки персональных данных.

# ОБЪЕМ И КАТЕГОРИИ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ, КАТЕГОРИИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Объем персональных данных, обрабатываемых в Банке, определяется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», требованиями внутренних документов Банка.
	2. В Банке не осуществляется обработка специальных категорий персональных данных, в соответствии со ст.10 Федерального закона от 27.07.2006 № 152-ФЗ касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни.
	3. В Банке не осуществляется обработка биометрических данных, на основании которых можно установить личность человека, в соответствии со ст.11 Федерального закона от 27.07.2006 № 152-ФЗ.
	4. Оператор осуществляет трансграничную передачу персональных данных в случаях, установленных действующим законодательством Российской Федерации, а также в целях исполнения договора, стороной которого является субъект персональных данных.
	5. В зависимости от субъекта персональных данных, Банк обрабатывает персональные данные следующих категорий персональных данных:
* персональные данные работника Банка - информация, необходимая Банку в связи с трудовыми отношениями и касающаяся конкретного работника;
* персональные данные аффилированного лица, инсайдера или персональные данные руководителя, участника (акционера) или работника юридического лица, являющегося аффилированным лицом по отношению к Банку - информация, необходимая Банку для отражения в отчетных документах о деятельности Банка в соответствии с требованиями федеральных законов, нормативных документов Банка России и иных нормативных правовых актов;
* персональные данные клиента, а также персональные данные руководителя, участника (акционера) или работника юридического лица, являющегося клиентом Банка-информация, необходимая Банку для выполнения своих обязательств в рамках договорных отношений с клиентом и для выполнения требований законодательства Российской Федерации;
* персональные данные потенциального клиента, контрагента, заемщика - информация, необходимая Банку в целях рассмотрения вопроса о заключении договорных отношений /проведении операций и сделок с потенциальным клиентом, контрагентом, заемщиком и для выполнения требований законодательства Российской Федерации;
* персональные данные представителя клиента – информация, необходимая Банку для выполнения своих обязательств в рамках договорных отношений с клиентом и для выполнения требований законодательства Российской Федерации.

# ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
	2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
	3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
	4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
	5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
	6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных.
	7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством Российской Федерации, либо договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Хранение персональных данных осуществляется Оператором на территории Российской Федерации.
	8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством Российской Федерации.

# УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 N 152-ФЗ. Обработка персональных данных осуществляется Оператором в следующих случаях:
1. обработка персональных данных осуществляется с согласия субъекта на обработку его персональных данных;
2. обработка персональных данных необходима для осуществления и выполнения функций, полномочий и обязанностей, возложенных на Оператора действующим законодательством Российской Федерации;
3. обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
4. обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с действующим законодательством Российской Федерации об исполнительном производстве;
5. обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, в т. ч. в случае реализации Оператором своего права на уступку прав (требований) по такому договору, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
6. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
7. обработка персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
8. обработка обезличенных персональных данных осуществляется в статистических целях;
9. осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;
10. осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с действующим законодательством Российской Федерации.
	1. Оператор не осуществляет принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права или законные интересы, на основании исключительно автоматизированной обработки персональных данных.
	2. Оператор не осуществляет распространение персональных данных, за исключением случаев, прямо предусмотренных действующим законодательством Российской Федерации.
	3. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством Российской Федерации, на основании заключаемого с этим лицом договора. Существенным условием такого договора является обязанность лица, осуществляющего обработку персональных данных по поручению Оператора, соблюдать принципы и правила обработки персональных данных, предусмотренные действующим законодательством Российской Федерации.
	4. Оператор осуществляет предоставление персональных данных представителям уполномоченных государственных органов в объеме и в порядке, установленном действующим законодательством Российской Федерации.

# ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

* 1. Субъект персональных данных принимает решение о предоставлении своих персональных данных Оператору и дает согласие на их обработку свободно, своей волей и в своем интересе.
	2. Субъект персональных данных имеет право на свободное и безвозмездное ознакомление с составом его персональных данных, обрабатываемых Оператором, получение информации, касающейся обработки его персональных данных, в том числе:
* подтверждение факта обработки персональных данных;
* правовые основания и цели обработки персональных данных;
* способы обработки персональных данных;
* наименование и место нахождения Оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Оператором или на основании действующего законодательства Российской Федерации;
* обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен действующим законодательством Российской Федерации;
* сроки обработки персональных данных, в том числе сроки их хранения;
* порядка осуществления субъектом персональных данных своих прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
* информация об осуществленной или о предполагаемой трансграничной передаче персональных данных;
* наименование или фамилия, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Оператора, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами за исключением случаев, установленных действующим законодательством Российской Федерации.
	1. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными или не являются необходимыми для заявленных целей обработки.
	2. Субъект персональных данных вправе требовать от Оператора извещения всех лиц, которым ранее передавались его персональные данные, обо всех произведенных в них дополнениях, исправлениях и исключениях.
	3. Субъект персональных данных вправе отозвать свое согласие на обработку персональных данных Оператором.
	4. Субъект персональных данных имеет также иные права, определенные главой 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

# ОБЯЗАННОСТИ ОПЕРАТОРА

* 1. При сборе персональных данных Оператор по запросу предоставляет субъекту информацию, указанную в п. 8.2 настоящей Политики.
	2. В случаях, когда предоставление персональных является обязательным в соответствии с действующим законодательством Российской Федерации, Оператор разъясняет субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
	3. Оператор не предоставляет третьим лицам и не распространяет персональные данные без согласия субъекта персональных данных, если иное не предусмотрено действующим законодательством Российской Федерации.
	4. Оператор определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено действующим законодательством Российской Федерации.
	5. Оператор при обработке персональных данных принимает необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
	6. Оператор сообщает субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставляет возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.
	7. Оператор вносит изменения в персональные данные субъекта в срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными.
	8. Оператор уничтожает персональные данные субъекта в срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.
	9. Оператор вправе продолжить обработку персональных данных субъекта после отзыва им согласия на обработку его персональных данных в объеме, предусмотренном действующим законодательством Российской Федерации.
	10. Оператор выполняет также иные обязанности, определенные главой 4 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

# ПЕРЕЧЕНЬ МЕР, НАПРАВЛЕННЫХ НА ВЫПОЛНЕНИЕ ОБЯЗАННОСТЕЙ ОПЕРАТОРА

* 1. Оператор назначает лиц, ответственных за обработку персональных данных и за обеспечение информационной безопасности персональных данных.
	2. Оператор разрабатывает и утверждает внутренние нормативные документы по вопросам обработки и обеспечения информационной безопасности персональных данных.
	3. Оператор осуществляет внутренний контроль и (или) аудит соответствия обработки персональных данных требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, внутренним нормативным документам Оператора.
	4. Оператор осуществляет оценку вреда, который может быть причинен субъектам в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также соотношения указанного вреда и принимаемых Оператором мер, направленных на обеспечение выполнения своих обязанностей.
	5. Оператор осуществляет ознакомление своих работников, осуществляющих обработку персональных данных, с законодательными актами Российской Федерации, нормативными документами Банка России, внутренними нормативными документами по вопросам обработки и обеспечения информационной безопасности персональных данных.
	6. Оператор осуществляет учет информационных систем персональных данных, мест хранения и обработки персональных данных (в том числе машинных носителей информации), а также учет работников, осуществляющих обработку персональных данных.
	7. Оператор определяет актуальные угрозы безопасности персональных данных при их обработке в ИСПДн. В соответствии с выявленными актуальными угрозами безопасности персональных данных Оператор внедряет комплекс организационных и технических мер, позволяющий нейтрализовать указанные угрозы.
	8. Оператор проводит оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационных систем персональных данных.
	9. Оператор устанавливает правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечивает регистрацию и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.
	10. Оператор внедряет средства минимизации полномочий доступа, разграничения доступа, мониторинга и контроля событий, обнаружения фактов неправомерного доступа, а также средства защиты информации, в том числе средства криптографической защиты информации, прошедшие в установленном порядке процедуру оценки соответствия.
	11. Оператор разрабатывает и внедряет меры реагирования на инциденты информационной безопасности в отношении персональных данных, а также меры по восстановлению персональных данных, модифицированных или уничтоженных вследствие неправомерного доступа к ним.

# ОТВЕТСТВЕННОСТЬ ОПЕРАТОРА

* 1. Контроль исполнения требований настоящей Политики осуществляется Ответственным за организацию обработки персональных данных.
	2. Лица, виновные в нарушении требований настоящей Политики, несут предусмотренную законодательством Российской Федерации ответственность.

# РАСКРЫТИЕ ИНФОРМАЦИИ

* 1. Обеспечение реализации прав субъектов персональных данных осуществляется посредством исполнения запросов, направляемых субъектами Оператору по адресам:
	+ почтовый адрес: Российская Федерация, 187015, Ленинградская область, Тосненский район, городское поселение Красный Бор, ул. Промышленная, д.3, пом. II;
	+ электронный адрес: oper@bereit.ru.
	1. Настоящая Политика подлежит публикации на официальном представительстве Оператора в сети Интернет (web-сайте) по адресу <http://bereit.ru/>. Доступ к настоящей Политике для ознакомления с ней предоставляется неограниченному кругу лиц.