



КРЕДИТ УРАЛ БАНК

ГРУППА ГАЗПРОМБАНКА

(Акционерное общество)

УТВЕРЖДЕНО
РЕШЕНИЕМ ПРАВЛЕНИЯ
БАНКА «КУБ» (АО)
Протокол № _____
от «___» _____ 2025 г.

ПОЛИТИКА

**в отношении защиты и обработки
персональных данных**

**«Кредит Урал Банк»
(Акционерное общество)**

г. Магнитогорск

ОГЛАВЛЕНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ	3
2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	3
3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	4
4. ОБЪЕМ И КАТЕГОРИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ	5
5. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	8
6. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	10
7. ОРГАНИЗАЦИЯ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	11
8. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ	14
9. МЕРЫ БАНКА, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	15
10. ПОРЯДОК УВЕДОМЛЕНИЯ ОБ ИНЦИДЕНТАХ	16
11. ОТВЕТСТВЕННОСТЬ.....	18
12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	18

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Политика в отношении защиты и обработки персональных данных (далее – Политика) определяет политику «Кредит Урал Банк» (Акционерное общество) (далее – Банк) в отношении обработки и обеспечения безопасности персональных данных.

1.2 Настоящая Политика разработана в соответствии с действующим законодательством Российской Федерации в области защиты персональных данных и направлена на обеспечение 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.

1.3 Целью настоящей Политики являются определение особенностей осуществления обработки и обеспечения безопасности персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152 «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

1.4 Настоящая Политика распространяется на все технологические процессы Банка, связанные с обработкой персональных данных субъектов, и обязательна для применения всеми работниками Банка.

1.5 Банк включен в реестр операторов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Регистрационный номер Банка в реестре – 12-0243666.

1.6 Требования настоящей Политики, при необходимости, могут детализоваться иными внутренними нормативными документами Банка.

1.7 В соответствии с требованиями ст. 18.1 Федерального закона от 27.07.2006 №152 «О персональных данных» настоящая Политика подлежит опубликованию в информационно-телекоммуникационной сети «Интернет».

2. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор информационной безопасности – должностное лицо, которое назначается Приказом Председателя Правления, ответственное за организацию обработки персональных данных, 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.

Банк – «Кредит Урал Банк» (Акционерное общество).

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

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 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.

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

Портал персональных данных – портал, предназначенный для информационного сопровождения деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети «Интернет» и его территориальных органов по защите прав субъектов персональных данных (<https://pd.rkn.gov.ru/incidents/>).

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

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Обработка персональных данных в Банке осуществляется на основе принципов:

- законности целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, определенным и заявленным при сборе персональных данных, а также полномочиям Банка;
- соответствия содержания и объема обрабатываемых персональных данных, способов обработки персональных данных, целям обработки персональных данных;
- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям их обработки, недопустимости избыточности обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- недопустимости объединения баз данных, содержащих персональные данные, для несовместимых между собой целей;
- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки или в случае утраты необходимости в достижении этих целей;
- уничтожения персональных данных по достижении целей обработки способом, исключающим возможность их восстановления.

3.2 Работники Банка, допущенные к обработке персональных данных, обязаны:

- знать и неукоснительно выполнять положения:
- законодательства Российской Федерации в области персональных данных;
- настоящей Политики;
- внутренних нормативных документов Банка по вопросам обработки персональных данных;
- обрабатывать персональные данные только в рамках выполнения своих должностных обязанностей;
- не разглашать персональные данные, обрабатываемые в Банке;
- сообщать о действиях других лиц, которые могут привести к нарушению положений настоящей Политики;

– сообщать об известных фактах нарушения требований настоящей Политики Администратору информационной безопасности.

3.3 Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

3.4 Сроки обработки персональных данных определяются в соответствии с целями их обработки, требованиями законодательства Российской Федерации и нормативными документами Банка России.

3.5 При достижении цели обработки персональных данных Банк прекращает обработку персональных данных или обеспечивает ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) и уничтожает персональные данные или обеспечивает их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Банком и субъектом персональных данных либо если Банк не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152 «О персональных данных».

3.6 При определении состава обрабатываемых персональных данных субъектов персональных данных Банк руководствуется минимально необходимым составом персональных данных для достижения целей получения персональных данных.

3.7 Безопасность персональных данных в Банке обеспечивается выполнением согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и работы информационных систем персональных данных в случае реализации угроз.

4. ОБЪЕМ И КАТЕГОРИЯ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Банком осуществляется обработка персональных данных, полученных в установленном законом порядке, следующих субъектов персональных данных:

- акционеры/участники;
- физические лица, аффилированные с Банком;
- физические лица, входящие в органы управления Банка;
- физические лица, которым оформляются пропуска на территорию мест нахождения Банка;
- физические лица и индивидуальные предприниматели, их законные представители, намеревающиеся вступить или состоящие в договорных и иных гражданско-правовых отношениях с Банком, в том числе через партнеров или контрагентов Банка (лица оказывающие услуги Банку, заемщики, залогодатели, поручители, вкладчики, владельцы банковских счетов, лица, арендующие банковские сейфовые ячейки,

отправители-получатели платежей и иные лица, пользующиеся финансовыми услугами Банка), иные лица, обработка персональных данных которых необходима для возникновения и/или исполнения указанных договорных и иных гражданско-правовых отношений (супруг/супруга заемщика, поручителя, залогодателя, опекуна, наследник(-и) и т.п.)

- физические лица, состоящие в гражданско-правовых отношениях с Клиентом Банка, в интересах которого Клиент осуществляет финансовые операции (платежи);

- физические лица - представители юридических лиц, уполномоченные взаимодействовать с Банком, в том числе в связи с намерением вступить или состоящие в договорных и иных гражданско-правовых отношениях с Банком;

- выгодоприобретатели;

- бенефициарные владельцы;

- пользователи сайта;

- лица, персональные данные которых передаются в Банк в рамках оказания финансовых услуг, исполнения договора с третьими лицами, прямых сделок купли-продажи имущества;

- работники, находящиеся в трудовых отношениях с Банком,

- физические лица, осуществляющие выполнение работ по оказанию услуг и заключившие с Банком договор гражданско-правового характера;

- бывшие работники Банка;

- физические лица, направившие резюме при устройстве на работу, для участия в конкурсе на замещение вакантных должностей;

- стажеры, практиканты;

- близкие родственники работников;

- физические лица, обратившиеся (обращавшиеся) в Банк с жалобами, заявлениями;

- работники, представители федеральных, региональных органов государственной власти РФ, органов местного самоуправления, судов, правоохранительных органов и других регуляторов;

- работники, члены Российских и международных организаций, отраслевых ассоциаций, Международных платежных систем и других коммерческих и некоммерческих организаций, а также представители средств массовой информации;

- участники конкурсов по выбору поставщиков продукции и услуг;

- лица, осуществляющие доставку корреспонденции (курьеры, сотрудники спецсвязи, Почты России);

- иные физические лица, выразившие согласие на обработку Банком их персональных данных или физические лица, обработка персональных данных которых необходима Банку для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения возложенных законодательством РФ на Банк функций, полномочий и обязанностей.

4.2 При определении состава обрабатываемых персональных данных субъектов персональных данных Банк руководствуется минимально необходимым перечнем персональных данных для достижения целей обработки персональных данных.

4.3 В состав обрабатываемых персональных данных могут входить:

- Фамилия, имя, отчество (при наличии);

- Фамилия при рождении;
- Фамилия, имя, отчество (при наличии) супруга(-и);
- Пол;
- Дата рождения (число, месяц и год рождения);
- Место рождения, страна рождения;
- Адрес (проживания, пребывания, регистрации, постановки на учет, получения корреспонденции);
- Сведения о гражданстве, статус (резидент/нерезидент);
- Сведения о семейном положении, о составе семьи;
- Социальное положение (в том числе сведения о социальных льготах);
- Сведения о принадлежащем Клиенту имуществе;
- Сведения об опеке и попечительстве/ об усыновлении;
- Сведения об ИНН, СНИЛС, TIN;
- Данные миграционной карты;
- Данные документа, подтверждающего право на пребывание в РФ;
- Страна налогового резидентства;
- Контактные данные (телефон (домашний, мобильный), адрес электронной почты, почтовый адрес);
- Вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа и код подразделения органа (при наличии), выдавшего его, дата выдачи;
- Кредитная история;
- Номер счета, номер банковской карты;
- Постановление об опеке;
- Свидетельство о праве на наследство;
- Образование, профессия, должность, место работы, доходы (зарботная плата), сведения о трудовой деятельности;
- Сведения о дополнительном профессиональном образовании;
- Сведения о владении иностранными языками;
- Сведения о государственных наградах, иных наградах и знаках отличия;
- Сведения о воинском учете, реквизиты документов воинского учета, а также сведения, содержащиеся в документах воинского учета;
- Сведения об инвалидности, сроке действия установленной инвалидности;
- Сведения о состоянии здоровья;
- Сведения о наличии (отсутствии) судимости;
- Сведения о занятости Супруга(-и);
- Наименование должности и структурного подразделения, табельный номер, дата начала работы в организации, рабочий телефон;
- Фото и видеоизображения;
- Сведения, указанные в актах гражданского состояния;
- Сведения, указанные в свидетельстве о рождении детей;
- Количество иждивенцев;

- Биометрические персональные данные, обрабатываемые в случаях, предусмотренных ст. 14.1 ч. 9 Федерального закона от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации»;
- Сведения о посетителях сайта, cookie-файлы;
- IP-адрес в сети Интернет, используемый субъектом персональных данных для взаимодействия с Банком, в том числе для подключения к системе дистанционного банковского обслуживания, а также во время осуществления взаимодействия;
- Параметры устройства доступа к сервисам Банка;
- Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, Банком не осуществляется.
- Обработка сведений о состоянии здоровья осуществляется в соответствии с Трудовым кодексом, Федеральным законом «Об обязательном медицинском страховании в РФ», а также пунктом 2.3 части 2 статьи 10 Федерального закона от 27.07.2006 № 152 «О персональных данных»;
- Банк вправе осуществлять обработку биометрических персональных данных с целью идентификации Клиентов при оказании банковских услуг;
- Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных (или при отсутствии возможности оценки адекватности защиты), может осуществляться Банком исключительно в случаях исполнения договора, стороной которого является субъект персональных данных, либо при наличии согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных, либо в иных случаях, когда такая передача допускается в соответствии с положениями действующего законодательства о персональных данных.

5. ЦЕЛИ СБОРА И ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Обработка персональных данных, несовместимая с целями сбора персональных данных не допускается.

5.2 Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5.3 Обработка персональных данных осуществляется Банком для достижения следующих целей:

- осуществление банковских операций, услуг и иной деятельности, предусмотренной Уставом Банка, в соответствии с лицензией Банка России, выданной Банку, действующим законодательством Российской Федерации, нормативными актами Банка России;
- рассмотрение возможности предоставления финансовых или иных услуг субъекту персональных данных в соответствии с законодательством РФ;
- предоставление отчетности государственным надзорным органам, Банку России в соответствии с требованиями действующего законодательства РФ;
- предоставление субъекту персональных данных информации об оказываемых услугах, о разработке Банком новых продуктов и услуг, об услугах партнеров Банка,

информирование о предложениях по продуктам и услугам, а также о проводимых акциях, об оценке качества обслуживания клиентов и мероприятиях (по которым имеется предварительное согласие Клиента на их получение);

- проведение мероприятий по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД ФТ);
- формирование и получение данных о кредитной истории Клиента;
- заключение, исполнение и прекращение договоров с физическими и юридическими лицами Клиентами и контрагентами и/или реализация совместных проектов;
- проведение мероприятий, необходимых действий по урегулированию заявлений, претензий; обработке сообщений Клиентов по вопросам качества обслуживания, предоставления продуктов, деятельности каналов продаж;
- обработка запросов субъектов персональных данных (в рамках действующего законодательства РФ);
- обеспечение пропускного режима на объектах Банка;
- выявление случаев мошенничества, хищения денежных средств со счета Клиента, иных противоправных действий, предотвращения таких противоправных действий в дальнейшем и локализации последствий таких действий;
- прием на практику студентов и выпускников учебных заведений для прохождения ознакомительной, учебной, производственной или преддипломной практики, а также для ознакомления с работой подразделений Банка и дальнейшее рассмотрение практиканта как кандидата на открытые вакансии Банка;
- рассмотрение возможности заключения, заключение и исполнение трудового соглашения/договора с субъектом персональных данных;
- регулирование трудовых (гражданско-правовых) отношений субъекта персональных данных с Банком (обеспечение соблюдения законов и иных нормативных правовых актов, ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении, продвижении по службе, пользовании различного вида льготами в соответствии с законодательством РФ, направление на медицинский осмотр, организация командировок, исполнение санитарно-противоэпидемических (профилактических) целей);
- размещение информации о работниках Банка на официальном сайте, досках почета, вывешенных в служебных помещениях Банка, внутреннем информационном портале Банка, Личном кабинете Работника Банка, системе электронного документооборота Банка;
- передача Банком персональных данных или поручение их обработки третьим лицам в соответствии с действующим законодательством РФ;
- осуществление мероприятий по проверке контрагента/Клиента (лица, осуществляющего функции единоличного исполнительного органа юридического лица/его уполномоченных представителей/учредителей/бенефициарных владельцев) до заключения с ними договора;
- осуществление телефонной связи с целью информирования о задолженности перед Банком (в том числе о сумме и сроках погашения задолженности);
- взыскание просроченной/проблемной задолженности;

- получение и обработка сведений, содержащихся в индивидуальном лицевом счете в Социальном Фонде России (СФР);
- информирование Клиента о проведенных операциях;
- регистрация субъекта персональных данных в Единой биометрической системе;
- исполнение поручения третьего лица на обработку персональных данных в соответствии с требованиями действующего законодательства РФ;
- осуществление других функций, полномочий и обязанностей, возложенных на Банк действующим законодательством Российской Федерации.

5.4 В целях анализа поведения посетителей сайта на сайте, а также анализа эффективности используемых в сети Интернет средств рекламы и продвижения ресурса, а также для целей оптимизации Банком своих веб-ресурсов, Банк самостоятельно обрабатывает обезличенные сведения о посетителях сайта (количество посетителей сайта, количество визитов на сайт, среднее время, проведенное на сайте за визит, запрошенный контент сайта, поведение на сайте, глубина просмотра и т.д.), а также с помощью аналитических интернет-сервисов. Посетители сайта заранее уведомляются о такой обработке и, в случае несогласия с ней, могут покинуть сайт Банка. В этом случае их данные не обрабатываются.

6. ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Обработка персональных данных осуществляется Банком в соответствии с требованиями законодательства Российской Федерации.

6.2 Обработка персональных данных осуществляется с согласия субъектов персональных данных на обработку их персональных данных, а также без такового в случаях, предусмотренных законодательством Российской Федерации.

6.3 Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой, позволяющей подтвердить факт его получения форме, если иное не установлено законодательством Российской Федерации.

6.4 Обработка персональных данных осуществляется в соответствии с целями, заранее определенными и заявленными при сборе персональных данных, а также полномочиями Банка, определенными действующим законодательством Российской Федерации и договорными отношениями с работниками, клиентами и контрагентами Банка.

6.5 Персональные данные субъекта могут быть получены банком от лица, не являющегося субъектом персональных данных, при условии предоставления банку подтверждения наличия оснований, указанных в п.п. 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона «О персональных данных» или иных оснований, предусмотренных законодательством РФ;

6.6 Банк осуществляет как автоматизированную, так и неавтоматизированную обработку персональных данных.

6.7 В случае выявления неправомерной обработки Персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя, либо уполномоченного органа по защите прав субъектов персональных данных Банк осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных

данных с момента такого обращения или получения указанного запроса на период проверки.

6.8 В случае подтверждения неправомерной обработки персональных данных, Банк в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные. Документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных, в случае если обработка персональных данных осуществлялась с использованием средств автоматизации.

6.9 В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в п. 6.8, Банк осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

6.10 Об устранении допущенных нарушений или об уничтожении персональных данных Банк уведомляет субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

6.11 Банк вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, на основании заключаемого с этим лицом договора, условием которого является соблюдение конфиденциальности и неразглашения персональных данных, а также требования к защите обрабатываемых персональных данных.

6.12 Право доступа к персональным данным субъектов персональных данных на бумажных и электронных носителях имеют работники Банка в соответствии с их должностными обязанностями.

6.13 Персональные данные не раскрываются третьим лицам и не распространяются иным образом без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

6.14 Представители органов государственной власти (в том числе, контролирующих, надзорных, правоохранительных и иных органов), получают доступ к персональным данным, обрабатываемым в Банке, в объеме и порядке, установленном законодательством Российской Федерации.

7. ОРГАНИЗАЦИЯ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Банк осуществляет передачу персональных данных государственным органам и уполномоченным юридическим и физическим лицам в рамках их полномочий и компетенции в соответствии с Федеральным законом от 27.07.2006 № 152 «О персональных данных» в следующих случаях:

- передача персональных данных осуществляется в рамках функций, обязанностей и полномочий, возложенных на Банк законодательством Российской Федерации;

- передача персональных данных необходима для осуществления прав и законных интересов Банка или третьих лиц, при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- передача персональных данных осуществляется в рамках исполнения или в целях заключения по инициативе субъекта персональных данных договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;

- передача персональных данных осуществляется с согласия субъекта персональных данных на передачу его персональных данных (в письменной или любой форме, в зависимости от категории передаваемых персональных данных);

- передача персональных данных осуществляется с согласия субъекта персональных данных при поручении Банком обработки персональных данных третьему лицу, если иное не предусмотрено федеральным законом;

- в иных случаях, предусмотренных Федеральным законом от 27.07.2006 № 152 «О персональных данных», иными федеральными законами.

7.2 Договор, предусматривающий передачу персональных данных (за исключением случаев, когда Банк дает поручение на обработку персональных данных), должен содержать следующие обязательства сторон:

- обрабатывать персональные данные исключительно в целях и способами, необходимыми для заключения и исполнения договора, предусматривающего передачу персональных данных;

- соблюдать принципы и правила обработки персональных данных, предусмотренные законодательством Российской Федерации;

- обеспечивать конфиденциальность и безопасность персональных данных;

- принимать (обеспечивать принятие) необходимых мер для защиты персональных данных;

- обеспечивать законные основания для передачи принимающей стороне персональных данных и совершения принимающей стороной действий по обработке персональных данных, необходимых для исполнения договора, в отношении полученных от передающей стороны персональных данных;

- обязанность уведомления передающей стороной субъекта персональных данных об осуществлении обработки его персональных данных принимающей стороной в рамках договора, предусматривающего передачу персональных данных, если сторонами не был определен иной порядок уведомления субъекта персональных данных.

7.3 Банк при передаче персональных данных руководствуется следующими правилами:

- несанкционированный доступ к персональным данным в процессе передачи должен быть исключен;

- передача персональных данных возможна только в том случае, если обеспечивается конфиденциальность и безопасность передаваемой информации;

- ограничивать передаваемую информацию только теми персональными данными, которые необходимы получающей стороне для достижения целей передачи персональных данных.

7.4 Банк, являясь оператором персональных данных, вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное

не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора.

7.5 В поручении на обработку персональных данных должны быть определены:

- категории субъектов персональных данных, обработку персональных данных которых Банк поручает третьему лицу;
- перечень персональных данных;
- перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных;
- цели обработки персональных данных;
- требования к защите обрабатываемых персональных данных, установленные Федеральным законом от 27.07.2006 № 152 «О персональных данных»;
- порядок уничтожения персональных данных.

7.6 В поручении на обработку персональных данных устанавливается обязанность лица, осуществляющего обработку персональных данных по поручению Банка:

- соблюдать конфиденциальность персональных данных;
- обеспечивать безопасность персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152 «О персональных данных» при их обработке;
- в случае сбора персональных данных обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации;
- принимать меры, направленные на обеспечение выполнения обязанностей оператора, возложенных Федеральным законом от 27.07.2006 № 152 «О персональных данных»;
- предоставлять документы и иную информацию по запросу Банка, подтверждающие принятие мер и соблюдение требований по обработке и защите персональных данных, установленных в поручении на обработку персональных данных с учетом законодательства Российской Федерации;
- безотлагательно уведомлять Банк о случаях установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

7.7 Требования к поручению на обработку персональных данных разрабатываются лицом, ответственным за организацию обработки персональных данных в Банке и утверждаются приказом Банка.

7.8 Банк может осуществлять трансграничную передачу персональных данных при наличии у него законных оснований для такой передачи. Решение о запрещении либо об ограничении трансграничной передачи персональных данных на территорию конкретного иностранного государства, конкретному органу власти иностранного государства или иностранному юридическому или физическому лицу принимается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

8. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

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

8.2 Субъект персональных данных имеет право на получение информации касающейся обработки его персональных данных, в соответствии с требованиями ст. 14 Федерального закона №152 «О персональных данных».

8.3 Субъект персональных данных, если иное не предусмотрено требованиями законодательства Российской Федерации, имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных Банком;
- правовые основания и цели обработки персональных данных;
- цели и применяемые Банком способы обработки персональных данных;
- наименование и местонахождение Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Банком или на основании федерального закона;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных и источник их получения Банком, если иной порядок представления персональных данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе, сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом №152 «О персональных данных»;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Банка, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные Федеральным законом № 152 «О персональных данных» или другими федеральными законами.

8.4 Порядок направления субъектом персональных данных (его представителем) запросов на предоставление сведений определен требованиями Федерального закона № 152 «О персональных данных». В частности, в соответствии с указанными требованиями запрос на получение информации в Банке должен содержать:

- серию, номер основного документа, удостоверяющего личность субъекта персональных данных (его представителя), сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта персональных данных в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Банком;
- подпись субъекта персональных данных (его представителя).

8.5 Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8.6 Запросы и обращения субъектов или их представителей регистрируются в соответствии с Регламентом ведения работы с обращениями, поступающими в Банк «Куб» (АО).

8.7 Банк предоставляет информацию, касающуюся обработки персональных данных субъекта, при обращении субъекта или его представителя в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Банк предоставляет безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных.

8.8 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, Банк вносит в них необходимые изменения. 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, Банк уничтожает такие персональные данные. Банк уведомляет субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принимает разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

8.9 Субъекты персональных данных несут ответственность за предоставление Банку достоверных сведений, а также за своевременное обновление предоставленных данных в случае каких-либо изменений.

8.10 Субъект персональных данных имеет также иные права, установленные Федеральным законом № 152 «О персональных данных».

9. МЕРЫ БАНКА, НАПРАВЛЕННЫЕ НА ОБЕСПЕЧЕНИЕ ВЫПОЛНЕНИЯ ОБЯЗАННОСТИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1 Банк при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие 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.

9.2 Банк самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения требований законодательства Российской Федерации. Банк принял следующие меры:

- назначен Администратор информационной безопасности;
- издаются внутренние нормативные документы Банка по вопросам обработки персональных данных, а также внутренние нормативные документы, устанавливающие

процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- определяются угрозы безопасности персональных данных при их обработке в информационных системах персональных данных;

- проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации;

- применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- обработка персональных данных без использования средств автоматизации осуществляется таким образом, что в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- осуществляется раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- осуществляется принятие мер в целях исключения фактов несанкционированного доступа к персональным данным;

- устанавливаются правила доступа к персональным данным, обрабатываемым в информационных системах;

- внедряются и применяются средства минимизации полномочий доступа, средства разграничения доступа (идентификация и аутентификация субъектов доступа, ограничения количества неудачных попыток доступа) и другие меры защиты.

- осуществляется внутренний контроль соответствия обработки персональных данных Федеральному закону № 152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Банка в отношении обработки персональных данных, локальным актам Банка;

- работники Банка, непосредственно осуществляющие обработку и организующие защиту персональных данных, изучают документы, определяющие политику Банка в отношении обработки персональных данных, внутренние нормативные документы по вопросам обработки персональных данных;

- при осуществлении хранения персональных данных Банк использует базы данных, находящиеся на территории Российской Федерации, в соответствии с ч. 5 ст. 18 Федерального закона от 27.07.2006 №152 «О персональных данных»;

- осуществляется периодическая (ежегодная) проверка точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных.

10. ПОРЯДОК УВЕДОМЛЕНИЯ ОБ ИНЦИДЕНТАХ

10.1 Уведомление об инциденте в области персональных данных осуществляется Банком в соответствии с требованиями законодательства Российской Федерации.

10.2 Банк в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, с момента выявления такого инцидента Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте (первичное уведомление);
- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента (дополнительное уведомление).

10.3 Порядок направления уведомления об инциденте определен требованиями Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций №187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

10.4 Первичное уведомление об инциденте должно содержать:

- о произошедшем инциденте (дату и время выявления инцидента, характеристику (характеристики) персональных данных (содержание базы данных, ставшей доступной неограниченному кругу лиц в результате неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, количество содержащихся в ней записей. Дополнительно Банк может представить информацию об актуальности скомпрометированной базы данных, а также о периоде, в течение которого собраны персональные данные);
- о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных (предварительные причины неправомерного распространения персональных данных, повлекшего нарушение прав субъектов персональных данных);
- о предполагаемом вреде, нанесенном правам субъектов персональных данных (результаты предварительной оценки вреда, который может быть нанесен субъектам персональных данных, в связи с неправомерным распространением персональных данных, а также последствия такого вреда);
- о принятых мерах по устранению последствий соответствующего инцидента (перечень принятых Банком организационных и технических мер по устранению последствий инцидента);
- о лице, уполномоченном Банком на взаимодействие с Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, по вопросам, связанным с выявленным инцидентом.

10.5 Дополнительное уведомление об инциденте должно содержать следующие сведения:

10.5.1 результаты внутреннего расследования выявленного инцидента:

- о причинах, повлекших нарушение прав субъектов персональных данных;
- о вреде, нанесенном правам субъектов персональных данных;
- о дополнительно принятых мерах по устранению последствий соответствующего инцидента (при наличии);

- о решении Банка о проведении внутреннего расследования с указанием его реквизитов).

10.5.2 информацию о лицах, действия которых стали причиной выявленного инцидента (при наличии):

- фамилия, имя, отчество (при наличии) должностного лица Банка с указанием должности (если причиной инцидента стали действия работника Банка);
- фамилия, имя, отчество (при наличии) физического лица, индивидуального предпринимателя или полное наименование юридического лица, действия которых стали причиной выявленного инцидента;
- IP-адрес компьютера или устройства;
- предполагаемое местонахождение таких лиц и (или) устройств (если причиной инцидента стали действия посторонних лиц);
- и иные сведения о выявленном инциденте, имеющиеся в распоряжении Банка.

10.6 С момента поступления уведомления, по адресу электронной почты, указанному в первичном уведомлении, Банку направляется информационное письмо, содержащее сведения о дате и времени передачи уведомления в информационную систему Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также номер и ключ уведомления. При направлении дополнительного уведомления посредством Портала персональных данных Банк указывает номер и ключ уведомления.

10.7 В случае если при направлении первичного уведомления Банк располагает сведениями о результатах внутреннего расследования выявленного инцидента, то он вправе указать такие сведения в первичном уведомлении.

10.8 Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа.

10.9 Уведомление в виде документа на бумажном носителе направляется по адресу Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. Уведомление в форме электронного документа направляется Банком посредством заполнения специализированной формы, размещенной на Портале персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций в информационно-телекоммуникационной сети «Интернет».

11. ОТВЕТСТВЕННОСТЬ

11.1 Контроль исполнения требований настоящей Политики в Банке осуществляется Администратором информационной безопасности.

11.2 Ответственность работников Банка, осуществляющих обработку персональных данных, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Банка.

12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

12.1. Настоящая Политика вступает в действие с момента утверждения.

12.2. Пункты настоящей Политики могут быть изменены с обязательным доведением до сведения работников Банка и опубликованием в информационно-телекоммуникационной сети «Интернет» новой редакции Политики.

12.3. В случае, если некоторые пункты данной Политики вступают в противоречие с законодательством Российской Федерации, нормативно-распорядительными документами Банка России, Уставом Банка, Политика остается действительной в части, не противоречащей вышеприведенным документам.

12.4. Политика подлежит периодическому (не реже 1 раза в год) пересмотру, а также актуализации в случае изменения нормативных, распорядительных документов или бизнес-процессов, затрагивающих область данной Политики.