



Утверждено решением Правления
ПРОТОКОЛ № 2024/06
ЗАСЕДАНИЯ ПРАВЛЕНИЯ
ООО «ГОЛДМАН САКС БАНК» от 25.04.2024

25 апреля 2024 г.

ООО «Голдман Сакс Банк»

**ПОЛИТИКА
ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ
ДАННЫХ ОБЩЕСТВА С ОГРАНИЧЕННОЙ
ОТВЕТСТВЕННОСТЬЮ
«ГОЛДМАН САКС БАНК»**

Версия 1.10

г. Москва
2024 г.

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Название документа	Политика обработки и обеспечения безопасности персональных данных Общества с ограниченной ответственностью «Голдман Сакс Банк»
Версия	1.10
Последнее обновление	25.04.2024
Владелец документа	Ответственный за организацию обработки персональных данных
Классификация	Общедоступный

ТАБЛИЦА ИЗМЕНЕНИЙ

Дата	Версия	Автор	Описание изменений
31.08.2018	1.0	Ответственный за организацию обработки персональных данных	Первоначальная версия
28.02.2019	1.1	Ответственный за организацию обработки персональных данных	Приложение № 1 исключено и утверждено в качестве отдельного документа
25.10.2019	1.2	Ответственный за организацию обработки персональных данных	Актуализация Политики в соответствии с фактическими процессами обработки
27.12.2019	1.3	Ответственный за организацию обработки персональных данных	Актуализация Политики в соответствии с фактическими процессами обработки
29.09.2020	1.4	Ответственный за организацию обработки персональных данных	Актуализация Политики в соответствии с фактическими процессами обработки
10.11.2020	1.5	Ответственный за организацию обработки персональных данных	Актуализация Политики в связи с изменением действующего законодательства

17.12.2020	1.6	Ответственный за организацию обработки персональных данных	Актуализация Политики в соответствии с фактическими процессами обработки
31.05.2021	1.7	Ответственный за организацию обработки персональных данных	Актуализация Политики в соответствии с фактическими процессами обработки
31.08.2022	1.8	Ответственный за организацию обработки персональных данных	Актуализация Положения в соответствии с фактическими процессами обработки и изменениями в законодательстве об обработке персональных данных
21.09.2023	1.9	Ответственный за организацию обработки персональных данных	Актуализация Положения в соответствии с фактическими процессами обработки
25.04.2024	1.10	Ответственный за организацию обработки персональных данных	Актуализация Положения в соответствии с фактическими процессами обработки, дополнено Приложением 1

СОДЕРЖАНИЕ

1.	ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	5
2.	ОБЩИЕ ПОЛОЖЕНИЯ.....	5
3.	ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БАНКОМ	5
4.	ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	6
6.	ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ	9
7.	СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	11
8.	АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ	11
9.	ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	12
10.	ПРАВА И ОБЯЗАННОСТИ БАНКА	14
11.	ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	14
12.	КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ И ЛОКАЛЬНЫХ АКТОВ БАНКА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ.....	15
13.	ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ	16

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Банк – оператор ПДн – Общество с ограниченной ответственностью «Голдман Сакс Банк», место нахождения: Российская Федерация, 125047, г. Москва, ул. Гашека, д. 6;

Закон о персональных данных – Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (с изменениями и дополнениями);

ИСПДн – информационная система ПДн, то есть совокупность содержащихся в базах ПДн и обеспечивающих их обработку информационных технологий и технических средств;

Материальный носитель – бумажные носители (оригиналы документов, содержащие ПДн; документы в печатной форме, полученные на основе информации, хранимой в информационных системах, – выписки, отчеты, и т.п.), а также электронные носители информации, в том числе отчуждаемые (USB flash, CD диски и т.п.);

ПДн – персональные данные, то есть любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (Субъекту ПДн);

Политика – настоящая Политика обработки и обеспечения безопасности персональных данных Общества с ограниченной ответственностью «Голдман Сакс Банк»;

Субъект ПДн – физическое лицо, ПДн которого обрабатываются Банком;

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

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая Политика определяет принципы, цели и условия обработки ПДн, стратегию и требования к их защите, а также основные права и обязанности оператора ПДн и Субъектов ПДн в Банке.

2.2. Настоящая Политика является основным руководящим локальным актом Банка, определяющим требования в отношении обработки и обеспечения безопасности ПДн.

2.3. Локальные акты Банка по вопросам, регулируемым настоящей Политикой, должны разрабатываться с учетом положений настоящей Политики и не противоречить им.

2.4. Настоящая Политика разработана в целях реализации положений законодательства Российской Федерации, требований иных нормативных правовых и методических документов в отношении обработки и защиты ПДн, а также защиты прав Субъектов ПДн.

3. ПРИНЦИПЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БАНКОМ

3.1. Обработка ПДн Банком осуществляется в соответствии с принципами:

- законности и справедливости целей и способов обработки ПДн;
- соответствия целей обработки ПДн законным целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Банка;
- соответствия объема и содержания обрабатываемых ПДн, а также способов обработки ПДн целям обработки ПДн;

- точности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;
- хранения ПДн в форме, позволяющей определить Субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, устанавливающий срок хранения федеральный закон или договор, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн;
- уничтожения ПДн после достижения целей их обработки, в случае утраты необходимости в достижении целей обработки или по окончании срока хранения ПДн, установленного федеральным законом или договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн.

4. ЦЕЛИ И ПРАВОВЫЕ ОСНОВАНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Банк осуществляет обработку ПДн в целях:

- исполнения прав и обязанностей сторон трудовых отношений в соответствии с трудовым законодательством;
- информационного обеспечения деятельности Банка;
- содействия в трудоустройстве;
- заключения и исполнения договоров добровольного медицинского страхования, страхования выезжающих за рубеж и при путешествии по территории Российской Федерации, договоров коллективного страхования жизни;
- согласования условий, заключения и исполнения договоров;
- коммуникации с бывшими работниками;
- обеспечения организации и реализации единых внутригрупповых бизнес-процессов группы Goldman Sachs;
- обеспечения соблюдения Банком применимого законодательства Российской Федерации, включая выполнение требований Федерального закона «О банках и банковской деятельности» от 2 декабря 1990 года № 395-1.

4.2. Если ПДн были собраны и обрабатываются для достижения определенной цели, для использования указанных ПДн в других целях Банк должен уведомить об этом Субъекта ПДн и, в случае необходимости, получить новое согласие на обработку ПДн.

4.3. Правовыми основаниями для обработки ПДн являются, в том числе:

- согласие Субъектов ПДн в соответствии с п. 1 ч. 1 ст. 6 Закона о персональных данных;
- договор, заключенный с Субъектом ПДн;
- достижение целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных

законодательством Российской Федерации на Банк функций, полномочий и обязанностей, в частности предусмотренным такими правовыми актами как:

- Гражданский кодекс Российской Федерации;
- Налоговый кодекс Российской Федерации;
- Трудовой кодекс Российской Федерации;
- Федеральный закон от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности»;
- Федеральный закон от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации доходов, полученных преступным путём, и финансированию терроризма»;
- Положение Банка России от 15 октября 2015 г. № 499-П «Об идентификации кредитными организациями клиентов, представителей клиента, выгодоприобретателей и бенефициарных владельцев в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- Федеральный закон от 27 июля 2010 г. № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»;
- Федеральный закон от 15 декабря 2001 г. № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;
- Федеральный закон от 24 июля 1998 г. № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний» ;
- Федеральный закон от 29 декабря 2006 г. № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»;
- Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;
- Федеральный закон от 25 июля 2002 г. № 115-ФЗ «О правовом положении иностранных граждан в Российской Федерации»;
- Федеральный закон от 18 июля 2006 г. № 109-ФЗ «О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации»;
- Федеральный закон от 28.03.1998 № 53-ФЗ «О воинской обязанности и военной службе»;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- «Основы законодательства Российской Федерации о нотариате» от 11.02.1993 № 4462-1;
- Закон Российской Федерации от 19.04.1991 № 1032-1 «О занятости населения в Российской Федерации»;
- Положение Банка России от 27 декабря 2017 г. № 625-П «О порядке согласования Банком России назначения (избрания) кандидатов на должности в финансовой организации, уведомления Банка России об избрании (прекращении полномочий), назначении (освобождении от должности) лиц, входящих в состав органов управления, иных должностных лиц в финансовых организациях, оценки соответствия квалификационным требованиям и (или) требованиям к деловой репутации лиц, входящих в состав органов управления, иных должностных лиц и учредителей (акционеров, участников) финансовых организаций, направления членом совета директоров (наблюдательного совета) финансовой организации информации в Банк России о голосовании (о непринятии участия в голосовании) против решения совета директоров (наблюдательного совета) финансовой организации, направления запроса о предоставлении Банком России информации и направления Банком России ответа о наличии (отсутствии) сведений в базах данных, предусмотренных статьями 75 и 76.7 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», а также о порядке ведения таких баз»;
- Указание Банка России от 25 декабря 2017 г. № 4662-У «О квалификационных требованиях к руководителю службы управления рисками, службы внутреннего контроля и службы внутреннего аудита кредитной организации, лицу, ответственному за организацию системы управления рисками, и контролеру негосударственного пенсионного фонда, ревизору страховой организации, о порядке уведомления Банка России о назначении на должность (об освобождении от должности) указанных лиц (за исключением контролера негосударственного пенсионного фонда), специальных должностных лиц, ответственных за реализацию правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма кредитной организации, негосударственного пенсионного фонда, страховой организации, управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, микрофинансовой компании, сотрудника службы внутреннего контроля управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, а также о порядке оценки Банком России соответствия указанных лиц (за исключением контролера негосударственного пенсионного фонда) квалификационным требованиям и требованиям к деловой репутации»;
- Указание Банка России от 28 декабря 2015 г. № 3921-У «О составе, объеме, порядке и сроках раскрытия информации профессиональными участниками рынка ценных бумаг».

5. ОБРАБАТЫВАЕМЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

5.1. Банк обрабатывает ПДн следующих Субъектов ПДн:

- кандидатов на замещение вакантных должностей;
- родственников кандидатов на замещение вакантных должностей;

- рекомендателей;
- работников;
- бывших работников;
- родственников работников;
- лиц, входящих в состав органов управления, и иных должностных лиц Банка (за исключением членов Совета директоров);
- членов Совета директоров Банка;
- единоличного исполнительного органа участников Банка и лиц, устанавливающих (осуществляющих) контроль в отношении участников Банка;
- представителей компаний, оказывающих Банку услуги, поставщиков, консультантов и аналогичных контрагентов;
- контактных лиц клиентов и контрагентов;
- проверяемых лиц клиентов;
- представителей государственных и муниципальных органов, регуляторов и саморегулируемых организаций.

5.2. Содержание и объем ПДн каждой категории Субъектов ПДн определяется необходимостью достижения конкретных целей их обработки, необходимостью Банка реализовать свои права и обязанности, а также права и обязанности соответствующего Субъекта ПДн.

5.3. Категории и перечень обрабатываемых ПДн, категории Субъектов, ПДн которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения ПДн при достижении целей их обработки или при наступлении иных законных оснований, Банк устанавливает сообразно каждой цели в Перечне персональных данных, утвержденным Правлением Банка, которое является Приложение 1 к настоящей Политике.

6. ПОРЯДОК И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка Банком ПДн осуществляется путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (предоставления, доступа), блокирования, удаления, уничтожения ПДн.

6.2. Обработка ПДн осуществляется путем смешанной (как автоматизированной, так и неавтоматизированной) обработки, в том числе с использованием внутренней корпоративной сети и сети Интернет.

6.3. Обработка Банком ПДн допускается в следующих случаях:

- обработка ПДн осуществляется на основании согласия Субъекта ПДн на обработку его ПДн;
- обработка ПДн необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения

возложенных законодательством Российской Федерации на Банк функций, полномочий и обязанностей;

- обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта органа государственной или муниципальной власти или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации;
- обработка ПДн необходима для исполнения договора, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн, а также для заключения договора по инициативе Субъекта ПДн;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом;
- в иных случаях, предусмотренных законодательством.

- 6.4. Источником всех ПДн является Субъект ПДн. Если иное не установлено законодательством, Банк вправе получать ПДн Субъекта ПДн от третьих лиц только при уведомлении об этом соответствующего Субъекта ПДн.
- 6.5. Банк вправе поручить обработку ПДн другому лицу с согласия соответствующего Субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключаемого с этой стороной договора (поручения на обработку ПДн). Лицо, осуществляющее обработку ПДн по поручению Банка, обязано соблюдать принципы и правила обработки ПДн, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.
- 6.6. В поручении третьему лицу Банком указываются перечень ПДн, перечень действий (операций) с ПДн, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели их обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных, требования, предусмотренные частью 5 статьи 18 и статьей 18.1 Закона о персональных данных, обязанность по запросу Банка в течение срока действия поручения Банка, в том числе до обработки ПДн, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение в целях исполнения поручения Банка требований, установленных в Законом о персональных данных, обязанность обеспечивать безопасность ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии со статьей 19 Закона о персональных данных, в том числе требование об уведомлении Банка о случаях, предусмотренных частью 3.1 статьи 21 Закона о персональных данных.
- 6.7. Банк может осуществлять Трансграничную передачу ПДн на территории иностранных государств при условии соблюдения действующих положений Закона о персональных данных.
- 6.8. При хранении ПДн в Банке соблюдаются условия, обеспечивающие сохранность и конфиденциальность ПДн.
- 6.9. Хранение ПДн осуществляется в форме, позволяющей идентифицировать Субъекта ПДн, но не дольше, чем этого требуют цели их обработки, если иной срок не установлен законодательством Российской Федерации или договором, стороной которого, выгодоприобретателем или поручителем по которому является Субъект ПДн.

7. СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Получение и обработка ПДн в случаях, предусмотренных Законом о персональных данных, осуществляется Банком с согласия Субъекта ПДн, в том числе в письменной форме.

7.2. Согласие Субъекта ПДн в письменной форме должно включать, в частности:

- фамилию, имя, отчество, адрес Субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование и адрес Банка;
- цель обработки ПДн;
- перечень ПДн, на обработку которых дается согласие Субъекта ПДн;
- наименование (фамилию, имя, отчество) и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка будет поручена такому лицу;
- перечень действий с ПДн, на совершение которых предоставляется согласие, общее описание используемых Банком способов обработки ПДн;
- срок, в течение которого действует согласие, а также способ его отзыва;
- подпись Субъекта ПДн.

7.3. Субъект ПДн дает Банку согласие на обработку своих ПДн свободно, в своей воле и своем интересе. Согласие на обработку ПДн может быть отозвано Субъектом ПДн путем направления в Банк заявления в свободной форме. В этом случае Банк обязуется прекратить обработку, а также уничтожить все имеющиеся в Банке ПДн Субъекта в сроки, установленные Законом о персональных данных, за исключением ПДн, которые Банк вправе обрабатывать без согласия Субъекта ПДн на иных законных основаниях.

7.4. Банк вправе обрабатывать ПДн без согласия Субъекта ПДн (или при отзыве Субъектом ПДн указанного согласия) при наличии оснований, указанных в п. 2-11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Закона о персональных данных, а также в иных случаях, предусмотренных законодательством.

8. АКТУАЛИЗАЦИЯ, ИСПРАВЛЕНИЕ И УНИЧТОЖЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. В случае обнаружения факта неточности ПДн или неправомерности их обработки, Банк обязан провести актуализацию или прекратить их обработку.

8.2. Обработка ПДн прекращается Банком в следующем порядке и сроки (если иное не предусмотрено законодательством Российской Федерации):

- при выявлении неправомерных действий с ПДн в срок, не превышающий трех рабочих дней с даты такого выявления, Банк устраняет допущенные нарушения. В случае невозможности устранения допущенных нарушений Банк в срок, не превышающий десяти рабочих дней с даты выявления неправомерности действий с ПДн, уничтожает ПДн. В случаях установленных Законом о персональных данных, об устранении допущенных нарушений или об уничтожении ПДн Банк уведомляет Субъекта ПДн или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным орган по защите прав Субъектов ПДн, также этот орган;

- при достижении цели обработки ПДн Банк прекращает обработку ПДн и уничтожает соответствующие ПДн в срок, не превышающий тридцати рабочих дней с даты достижения цели обработки ПДн;
- при отзыве Субъектом ПДн согласия на обработку своих ПДн Банк прекращает обработку ПДн и уничтожает (за исключением ПДн, которые хранятся в соответствии с действующим законодательством) ПДн в срок, не превышающий тридцати рабочих дней с даты поступления указанного отзыва.

8.3. В случае отсутствия возможности уничтожения ПДн в течение указанных сроков Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование и затем обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен законодательством Российской Федерации.

8.4. Уничтожение ПДн должно производиться способом, исключающим дальнейшую обработку этих ПДн.

8.5. В случае обращения Субъекта ПДн к Банку с требованием о прекращении обработки персональных данных Банк в срок, не превышающий 10 рабочих дней с даты получения Банком соответствующего требования, прекращает их обработку или обеспечивает прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку ПДн), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Закона о персональных данных. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес Субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

9. ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОТВЕТЫ НА ЗАПРОСЫ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

- подтверждение факта обработки ПДн Банком;
- правовые основания и цели обработки ПДн;
- цели и применяемые Банком способы обработки ПДн;
- наименование и местонахождение Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Банком или на основании федерального закона;
- перечень обрабатываемых ПДн Субъекта ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления Субъектом ПДн прав, предусмотренных Законом о персональных данных;
- информацию об осуществленной или о предполагаемой Трансграничной передаче ПДн;

- наименование (фамилию, имя, отчество) и адрес лица, осуществляющего обработку ПДн по поручению Банка, если обработка поручена или будет поручена такому лицу;
- информацию о способах исполнения Банком обязанностей, установленных статьей 18.1 Закона о персональных данных;
- иные сведения, предусмотренные Законом о персональных данных или другими федеральными законами.

9.2. Банк предоставляет указанную выше информацию на основании соответствующего письменного заявления Субъекта ПДн, направленного по адресу Банка: Российская Федерация, 125047, г. Москва, ул. Гашека, д. 6, или направленного на почтовый адрес Банка: Российская Федерация, 125047, г. Москва, ул. Гашека, д. 6. Заявление должно содержать номер основного документа, удостоверяющего личность Субъекта ПДн, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие Субъекта ПДн в отношениях с Банком (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн Банком, подпись Субъекта ПДн. Банк обязуется сообщить Субъекту ПДн информацию о наличии ПДн, относящихся к соответствующему Субъекту ПДн, в течение десяти рабочих дней с момента обращения либо получения Банком запроса Субъекта ПДн или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Банком в адрес Субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Банк предоставляет указанные сведения Субъекту ПДн или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

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

9.4. Субъект ПДн, давший Банку согласие на обработку ПДн, разрешенных Субъектом ПДн для распространения, вправе обратиться к Банку с требованием о прекращении передачи (распространения, предоставления, доступа) его ПДн. Соответствующее требование должно включать фамилию, имя, отчество (при наличии) Субъекта ПДн, его контактную информацию (номер телефона, адрес электронной почты или почтовый адрес), а также перечень ПДн, обработка которых подлежит прекращению. С момента поступления такого требования действие согласия на обработку ПДн, разрешенных Субъектом ПДн для распространения, прекращается, и Банк обязуется прекратить передачу (распространение, предоставление, доступ) указанных в требовании ПДн.

9.5. Если Субъект ПДн считает, что Банк осуществляет обработку его ПДн с нарушением требований законодательства, Субъект ПДн вправе обжаловать действия или бездействие Банка в уполномоченный орган по защите прав Субъектов ПДн или в судебном порядке.

9.6. Право Субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с федеральными законами Российской Федерации.

9.7. Субъект ПДн обязан:

- предоставлять Банку достоверные ПДн;
- своевременно сообщать Банку об изменениях и дополнениях своих ПДн;

- осуществлять свои права в соответствии с законом, иными нормативными правовыми актами и локальными актами Банка в области обработки и защиты ПДн;
- исполнять иные обязанности, предусмотренные законом, иными нормативными правовыми актами и локальными актами Банка в области обработки и защиты ПДн.

10. ПРАВА И ОБЯЗАННОСТИ БАНКА

10.1. При осуществлении обработки ПДн Банк вправе:

- устанавливать правила обработки ПДн в Банке, вносить изменения и дополнения в локальные акты, самостоятельно в рамках требований законодательства разрабатывать и применять формы документов, необходимых для исполнения обязанностей оператора ПДн;
- осуществлять иные права, предусмотренные законом, иными нормативными правовыми актами и локальными актами Банка в области обработки и защиты ПДн.

10.2. При осуществлении обработки ПДн Банк обязан:

- обеспечивать обработку ПДн исключительно в целях, для которых был осуществлен сбор ПДн;
- получать от Субъекта ПДн согласие на обработку его ПДн, в том числе в письменной форме, в случаях, установленных законодательством Российской Федерации;
- защищать ПДн от их неправомерного использования или утраты;
- исполнять иные обязанности, предусмотренные законодательством Российской Федерации и локальными актами Банка в области обработки и защиты ПДн.

10.3. Работники Банка, допущенные к работе с ПДн, несут персональную ответственность за обеспечение конфиденциальности полученных данных.

11. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

11.1. Банк не несет ответственность за раскрытие ПДн неограниченному кругу лиц по вине Субъекта ПДн.

11.2. Для обеспечения безопасности ПДн Банк принимает организационные и технические меры, в том числе включающие:

- назначение лица, ответственного за организацию обработки ПДн, определение его функций и полномочий;
- разработку и поддержание актуальности локальных актов в области обработки и защиты ПДн;
- оценку потенциального вреда, который может быть причинен Субъектам ПДн в случае нарушения Закона о персональных данных, а также соотношение потенциального вреда с принимаемыми мерами по обеспечению безопасности ПДн;

- ознакомление работников Банка, осуществляющих обработку ПДн, с положениями законодательства Российской Федерации и локальными актами Банка в области обработки и защиты ПДн, периодическое обучение вопросам обработки и защиты ПДн;
- определение угроз безопасности ПДн при их обработке в ИСПДн;
- учет работников, допущенных к обработке ПДн;
- учет машинных носителей ПДн;
- применение организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн;
- периодический внутренний контроль, а также аудит соответствия обработки ПДн требованиям Закона о персональных данных и принятым в соответствии с ним нормативным правовым актам;
- обнаружение фактов несанкционированного доступа к ПДн и принятие мер для устранения несанкционированного доступа и недопущения его в дальнейшем;
- восстановление ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к ПДн, обрабатываемым в ИСПДн, а также обеспечение регистрации и учета всех действий, совершаемых с ПДн в ИСПДн;
- контроль за принимаемыми мерами по обеспечению безопасности ПДн.

11.3. Комплекс мероприятий и технических средств по обеспечению безопасности ПДн в Банке устанавливается с учетом результатов оценки потенциального вреда Субъекту ПДн, который может быть нанесен в случае нарушения безопасности ПДн, актуальности угроз безопасности ПДн, а также установления уровня защищенности ПДн.

12. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ И ЛОКАЛЬНЫХ АКТОВ БАНКА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

12.1. Контроль за соблюдением локальных актов Банка в области обработки и защиты ПДн осуществляется с целью проверки соответствия процессов обработки и защиты ПДн требованиям законодательства Российской Федерации в области ПДн, а также выявления возможных каналов утечки и фактов несанкционированного доступа к ПДн.

12.2. Внутренний контроль за соблюдением структурными подразделениями Банка требований законодательства Российской Федерации и локальных актов Банка в области ПДн осуществляется лицом, ответственным за организацию обработки ПДн в Банке, совместно с руководителями структурных подразделений Банка либо назначенными ими ответственными работниками, на основании действующего законодательства и в соответствии с Правилами осуществления внутреннего контроля в области персональных данных Банка, утвержденными Правлением Банка.

12.3. Работники Банка, виновные в нарушении норм, регулирующих обработку и защиту ПДн, установленных в Банке, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной или уголовной ответственности в соответствии с законодательством Российской Федерации.

- 12.4. Банк обязан в порядке, определенном действующим законодательством, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн.
- 12.5. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов персональных данных, Банк обязан с момента выявления такого инцидента Банком, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомить уполномоченный орган по защите прав субъектов персональных данных:
- в течение 24 часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав Субъектов ПДн, и предполагаемом вреде, нанесенном правам Субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;
 - в течение 72 часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

13. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

- 13.1. Настоящая Политика является общедоступным документом и предоставляется для ознакомления неограниченному кругу лиц.
- 13.2. В своей деятельности члены органов управления, должностные лица и работники Банка руководствуются настоящей Политикой, а также иными внутренними документами Банка.
- 13.3. При несоответствии каких-либо положений настоящей Политики законодательству такие положения утрачивают силу. До момента внесения изменений в настоящую Политику Банк руководствуется соответствующими положениями законодательства Российской Федерации.
- 13.4. Банк вносит изменения в настоящую Политику в связи с изменениями во внутренних документах Банка, ИСПДн и системе защиты ПДн Банка.
- 13.5. Все работники Банка подлежат обязательному ознакомлению с настоящей Политикой и несут персональную ответственность за соблюдение настоящей Политики. Работники Банка обязаны доводить до сведения Председателя Правления Банка информацию обо всех известных им случаях нарушения требований настоящей Политики.