УТВЕРЖДЕНО
Правлением
“ИНТЕРПРОГРЕССБАНК”
(Акционерное общество)
Протокол № 12 от «08» апреля 2016 г.

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в “ИНТЕРПРОГРЕССБАНК” (Акционерное общество)

г. Москва.
2016 г.

Принятые сокращения:

Банк - “ИНТЕРПРОГРЕССБАНК” (Акционерное общество);
ПЭВМ - Персональная электронная вычислительная машина;
СКЗИ - Средства криптографической защиты информации;
АРМ - Автоматизированное рабочее место;
АИС - Автоматизированная информационная система;
АБС - Автоматизированная банковская система;
БД - База данных;
ОС - Операционная система;
ИСПДн – Информационная система персональных данных.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Сфера действия настоящего Положения

Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их автоматизированной и неавтоматизированной обработке в Банке, представляющих собой совокупность персональных данных, содержащихся в базах данных Банка, а также данных на материальных носителях.

Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах Банка.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.2. Цель настоящего Положения

Целью настоящего Положения является обеспечение конфиденциальности персональных данных при их обработке:

- исключение возможности несанкционированного доступа к персональным данным и использования этих данных работниками Банка и третьими лицами в собственных интересах в ущерб интересам клиентов Банка и интересам самого Банка;
- повышение уровня доверия к Банку со стороны клиентов;
- минимизация рисков предъявления претензий к Банку со стороны правоохранительных и иных государственных органов, а также юридических и физических лиц.

1.3. Основные понятия, используемые в настоящем Положении

В настоящем Положении используются следующие основные понятия:

▪ *персональные данные* - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, паспортные данные или данные иного документа, удостоверяющего личность, дата и место рождения, адрес, регистрация, семейное, социальное, имущественное положение, образование, профессия, данные трудовой книжки, доходы, другая информация, однозначно позволяющая идентифицировать личность;

▪ *оператор* - юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных;

▪ *обработка персональных данных* - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

▪ *распространение персональных данных* - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

▪ *использование персональных данных* - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

▪ *блокирование персональных данных* - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

▪ *уничтожение персональных данных* - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

▪ *обезличивание персональных данных* - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

▪ *информационная система персональных данных* - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

▪ *конфиденциальность персональных данных* - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

▪ *общедоступные персональные данные* - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.4. Законодательство о защите персональных данных

Законодательно-нормативная база по защите персональных данных включает в себя:

- Конституцию РФ (ст. 23, 24);

- Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (14 глава, с изменениями и дополнениями);
- Федеральный закон от 19.12.2005 № 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных";
- Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ "О персональных данных";
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 "Требования к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановление Правительства Российской Федерации от 06.07.2008 № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";
- Постановление Правительства Российской Федерации от 16.03.2009 № 228 "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций";
- Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
-Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 16 июля 2010 г. N 482 "Об утверждении образца формы уведомления об обработке персональных данных"
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 № 149/54-144);
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, от 21.02.2008 № 149/6/6-622).

На основании указанных выше документов Банком должен обеспечиваться требуемый уровень безопасности персональных данных.

2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Принципы обработки персональных данных

Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.
- хранения персональных данных, позволяющих определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки, с последующим уничтожением.

2.2. Условия обработки персональных данных

2.2.1. Обработка персональных данных может осуществляться Банком с согласия субъектов персональных данных, за исключением случаев, предусмотренных пунктом 2.2.2 настоящего Положения.

2.2.2. Согласия субъекта персональных данных, предусмотренного пунктом 2.2.1 настоящего Положения, не требуется в следующих случаях:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации ;

- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации ;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

- обработка персональных данных, сделанные общедоступными субъектом персональных данных.

2.2.3. В случае если Банк на основании договора поручает обработку персональных данных другому лицу, обязательным условием договора является обеспечение указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

2.3. Конфиденциальность персональных данных

Сотрудниками Банка и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных.

Обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

2.4. Общедоступные источники персональных данных

В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги и т.д.). Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных, либо по решению суда или иных уполномоченных государственных органов.

2.5. Согласие субъекта персональных данных на обработку своих персональных данных

Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

В случаях, предусмотренных Федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва.

Типовая форма согласия субъекта, на обработку его персональных данных представлена в Приложении №1.

3. ОБЯЗАННОСТИ ОПЕРАТОРА

3.1. Меры по обеспечению безопасности персональных данных при их обработке

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные.

3.2. Порядок обработки персональных данных, осуществляемой без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с законодательством Российской Федерации и "Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 N 687.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица,

осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.3. Принимаемые меры для защиты персональных данных

3.3.1. Организационные

- Размещение в разных помещениях сотрудников Банка, выполняющих различные виды профессиональной деятельности;
- Ограничение доступа посторонних лиц в помещения подразделений Банка, предназначенных для осуществления профессиональной деятельности;
- Размещение помещений подразделений Банка и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая работников других подразделений.
- Ограничение доступа посторонних лиц в помещения Банка после окончания рабочего дня;
- Ограничение доступа сотрудников и посторонних лиц в помещения Банка по выходным и праздничным дням;
- «Общие обязанности сотрудников Банка по обеспечению информационной безопасности при работе с АИС»;
- «Порядок обращения с информацией, подлежащей защите»;
- Приказ «Об ограничении доступа в помещение с установленным серверным и сетевым оборудованием»;
- Контроль за доступом в помещение с установленным серверным оборудованием;
- Служебные записки и заявки на доступ сотрудников Банка к работе в АБС, сети Интернет и с электронной почтой;
- «Положение по организации антивирусной защиты в автоматизированной системе Банка»;
- Приказ «О допуске сотрудников подразделений АБ «Интерпрогрессбанк» к выполнению деятельности, связанной с шифровальными средствами»;
- «Инструкция по работе с ключевыми дискетами в автоматизированной системе АБ «Интерпрогрессбанк»;
- Должностные инструкции сотрудников Банка;
- Приказ «О перечне сведений, составляющих коммерческую тайну Банка»;
- «Обязательство о неразглашении банковской и коммерческой тайны» (приложение к трудовому Договору).
- Инструкция по информационной безопасности;

- Модель угроз безопасности персональных данных при их обработке в ИСПДн в “ИНТЕРПРОГРЕССБАНК” (Акционерное общество). Указанная модель включает в себя список приемлемых для банка рисков.

3.3.2. Физические

- Физическая защита здания Банка и в т.ч. защита помещений;
- Пропускная система при входе в здание Банка;
- Разграничение доступа в кабинеты Банка;
- Размещение АРМ в контролируемых помещениях и разграничение доступа сотрудников к ним;
- Размещение серверного и сетевого оборудования в отдельном, контролируемом и запирающемся помещении;
- Наличие несгораемых сейфов для хранения ключевых носителей и документов;
- Использование жалюзи (штор) для защиты окон помещений, находящихся на первом этаже Банка, для предотвращения просмотра информации выведенной на экраны мониторов;
- Расположение мониторов ПЭВМ обрабатывающих персональные данные порядком, препятствующим визуальному считыванию посторонними лицами информации с экранов мониторов.

3.3.3. Технические

- Система контроля управления доступом;
- Пожарно-охранная сигнализация;
- Наличие запирающих устройств (замков) на дверях помещений и кабинетах Банка;
- Все двери помещений имеют разные замки;
- Наличие корпоративного межсетевого экрана (FireWall);
- Наличие корпоративного антивирусного экрана и анти-спам фильтра;
- Контроль и управление учетными записями в домене;
- Ограничение доступа пользователей к ресурсам сети Интернет;
- Наличие установленных паролей доступа на ПЭВМ пользователей;
- Разграничение прав доступа в ОС;
- Наличие антивирусных средств на ПЭВМ пользователей;
- Наличие при необходимости персональных межсетевых экранов на ПЭВМ пользователей;
- Наличие блокировки ОС при простое, с последующим обязательным вводом пароля для разблокировки системы;
- Использование шифровальных (криптографических) средств, для защиты персональных данных при передаче их по каналам связи;
- Разграничение доступа к электронным документам, хранящихся как на ПЭВМ пользователей, так и на серверах;
- Разграничение доступа сотрудников к работе с сервером системы, с программным обеспечением, с СКЗИ в соответствии с назначенными правами и полномочиями;
- Наличие парольной защиты при доступе к АБС;
- Разграничение прав доступа сотрудников к информации и функциям в АБС в соответствии с назначенными правами и полномочиями;
- Регистрация событий;
- Периодический отбор и удаление из БД информации, содержащей персональные данные утратившей актуальность;
- Плановое резервное копирование баз данных содержащих персональные данные и ограничение доступа к этим архивам.

3.4. Требования по обеспечению безопасности персональных данных

Каждый сотрудник Банка, участвующий в процессах обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным АБС, несет персональную ответственность за свои действия и обязан:

- Выполнять требования всех внутренних документов Банка, касающихся информационной безопасности;
- Соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АИС;
- Знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;
- Хранить в тайне свои аутентификационные реквизиты доступа;
- Соблюдать установленные правила обращения и хранения персональной ключевой дискеты;
- Отключать монитор своего персонального компьютера или блокировать вход в информационную систему в случае отлучения от своего рабочего места во время рабочего дня, в целях защиты от просмотра данных посторонними лицами, включая работников других подразделений;
- Выключать свою ПЭВМ после окончания рабочего дня;
- Закрывать двери рабочих кабинетов на ключ, в случае ухода из помещения в течение рабочего дня всех сотрудников. Также закрывать двери кабинетов после окончания рабочего дня.

3.5. Сотрудникам Банка запрещается:

- Осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- Обсуждать персональные данные с другими работниками Банка или иными лицами, не имеющими отношение к персональным данным;
- Записывать и хранить персональные данные на неучтенных носителях информации (диски, дискеты, флэш-накопители и другие съемные устройства);
- Оставлять без личного присмотра свою персональную ключевую дискету, магнитные носители и распечатки, содержащие персональные данные. Передавать посторонним лицам свою персональную ключевую дискету, делать неучтенные копии этой дискеты и вносить какие-либо изменения в файлы ключевой дискеты;
- Оставлять включенной без присмотра свою ПЭВМ, не предприняв необходимых мер защиты (отключение монитора, блокировка ОС, отключение ПЭВМ);
- Покидать свое рабочее место, оставляя без присмотра посторонних лиц рядом с носителями, содержащими сведения о персональных данных, включая работников других подразделений Банка.

4. КОНТРОЛЬ ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ. ОТВЕТСТВЕННОСТЬ ЗА ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

Контроль за соблюдением требований данного Положения осуществляет руководитель подразделения информационной безопасности (или сотрудник, выполняющий его обязанности) в виде просмотра и анализа отчетов, предоставляемых руководителями структурных подразделений при выявлении нарушений требований настоящего Положения (Приложение №2).

Ответственность за выполнение требований данного Положения возлагается на руководителей структурных подразделений Банка.

Сотрудники, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Приложение №1
К Положению об обеспечении безопасности персональных данных при их обработке в «ИНТЕРПРОГРЕССБАНК» (Акционерное общество)

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(ФИО полностью)

_____
(адрес регистрации по месту жительства)

_____

_____
(данные паспорта или иного документа, удостоверяющего личность)
(в т.ч сведения о дате выдачи указанного документа и выдавшем его органе)

не возражаю против обработки моих персональных данных, содержащихся в анкете, заявлении, а также в иных документах, предоставленных мной в **“ИНТЕРПРОГРЕССБАНК” (Акционерное общество), адрес: 115201, г. Москва, Старокаширское шоссе, дом 2, корпус 1**, и совершения с ними следующих действий: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу данных внутри Банка), обезличивание, блокирование, уничтожение персональных данных, при этом общее описание вышеуказанных способов обработки данных приведено в ФЗ №152 от 27.07.2006 г., а также право на передачу такой информации третьим лицам в случаях, предусмотренных действующим законодательством РФ, с целью *исполнения Банком требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», нормативными актами Банка России, принятия Банком решения при заключении трудового договора, рассмотрении моих заявок на предоставление банковских услуг, надлежащего оказания мне банковских услуг и исполнения Банком принятых на себя обязательств по заключенным со мною договорам.*

Настоящее согласие действует до даты его отзыва мною путем направления в Банк письменного сообщения об отзыве в произвольной форме, если иное не установлено законодательством Российской Федерации.

В случае не предоставления мной вышеуказанного письменного отзыва хранение моих персональных данных осуществляется в порядке и в течение срока, установленного Банком.

_____ _____ 20 _____ г. _____ _____
(подпись) *(ФИО)*

2. С обратной стороны Приложения №1 «Согласия на обработку персональных данных» размещается следующий текст:

ПАМЯТКА КЛИЕНТУ
(разработана в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»)

Уважаемый Клиент “ИНТЕРПРОГРЕССБАНК” (Акционерное общество)!

С 01.01.2010 г. в Российской Федерации начал действовать в полном объеме Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Согласно статьи 6 указанного закона обработка персональных данных может осуществляться Банком **только с согласия субъектов персональных данных.**

В соответствии со статьей 3 закона **персональными данными** является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Под **обработкой персональных данных** понимаются действия (операции) Банка с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространением персональных данных называются действия Банка, направленные на передачу персональных данных определенному кругу лиц. Касательно передачи персональных данных третьим лицам хочется обратить внимание, что данный вид обработки персональных данных осуществляется Банком с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа. **Круг третьих лиц, которым Банк имеет право передавать персональные данные, определен действующим законодательством и естественным образом ограничен целями, в которых осуществляется передача персональных данных. Это: – Банк России, государственные органы власти, иные организации, которые имеют право на получение персональных данных в соответствии с действующим законодательством.**

Основной целью обработки Банком персональных данных клиентов является:

- исполнение Банком требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», осуществления возложенных на Банк законодательством Российской Федерации функций в соответствии с Налоговым кодексом Российской Федерации, федеральными законами, в частности: «О банках и банковской деятельности», «О кредитных историях», «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «О валютном регулировании и валютном контроле», «О рынке ценных бумаг», «О несостоятельности (банкротстве) кредитных организаций», «О страховании вкладов физических лиц в банках Российской Федерации», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», нормативными актами Банка России;

- надлежащие оказание Клиенту банковских услуг и исполнение Банком принятых на себя обязательств по кредитным и депозитным договорам, договорам на открытие расчетных и карточных счетов и т.п.

Таким образом, информация о персональных данных необходима Банку для выполнения Ваших поручений на осуществление банковских операций и/или при заключении и/или исполнении договора на предоставление Вам соответствующей банковской услуги. Соответственно, клиент, не давший своего согласия на обработку персональных данных, лишается возможности получать банковские услуги. Сотрудники Банка не смогут включать персональные данные такого клиента в электронную карточку клиента и передавать эту информацию в соответствующие подразделения Банка, которым эта информация необходима в целях оказания клиенту необходимых банковских услуг. **Отказ от подписания согласия на обработку персональных данных фактически является добровольным отказом от получения банковских услуг в “ИНТЕРПРОГРЕССБАНК” (Акционерное общество).**

В связи с вышеизложенным Банк предлагает Вам подписать разработанную на основании п.4 ст. 9 ФЗ «О персональных данных» форму согласия на обработку персональных данных.

Банк, в свою очередь, на основании ст.19 ФЗ «О персональных данных» обязуется принять необходимые организационные и технические меры для защиты Ваших персональных данных от неправомерного или случайного доступа к ним третьих лиц, а также от иных неправомерных действий.

Требование об оформлении Согласия распространяется как на Клиентов, с которыми у Банка уже сложились отношения по оказанию банковских услуг и/или заключены соответствующие договоры, так и на Клиентов, впервые обратившихся в Банк с целью получения банковских услуг и/или заключения соответствующего договора.

Оформить Согласие на обработку Ваших персональных данных Вы можете у любого сотрудника операционного или клиентского отделов обслуживающего Вас Дополнительного офиса Банка и/или у руководителя (заместителя руководителя) того подразделения Банка, с которым Вы согласовываете условия заключаемого с Банком договора на оказание банковских услуг.

По вопросам, связанным с заполнением формы, Вы можете обратиться в Головной офис Банка по тел.: 8-495-411-00-00 или по телефону обслуживающего Вас Дополнительного офиса: _____ № _____.

Приложение №2
К Положению об обеспечении безопасности персональных данных при их обработке в «ИНТЕРПРОГРЕССБАНК» (Акционерное общество)

В Управление безопасности
“ИНТЕРПРОГРЕССБАНК”
(Акционерное общество)

Сведения о выявленных нарушениях

Подразделение банка _____

№ п/п	Выявленное нарушение	Дата (время) совершения нарушения	Кем выявлено нарушение	Принятые меры

_____ _____ _____
должность ФИО подпись

" _____ " _____ 20 __ г.