

ПОЛОЖЕНИЕ
об обработке персональных данных
в ПАО СКБ Приморья «Примсоцбанк».

г.Владивосток
2016 г.

Содержание.

1. Общие положения.	3
2. Термины и определения.....	4
3. Сокращения.....	5
4. Согласие на обработку персональных данных.....	5
5. Сроки обработки персональных данных.....	5
6. Поручение обработки персональных данных третьему лицу.	5
7. Трансграничная передача персональных данных.....	6
8. Обеспечение безопасности персональных данных, обрабатываемых с использованием средств автоматизации.	7
9. Обеспечение безопасности персональных данных, обрабатываемых без использования средств автоматизации.	7
10. Организация и управление доступом к персональным данным.	8
11. Обработка обращений и запросов.....	9
12. Хранение персональных данных.....	10
13. Уничтожение персональных данных.	9
14. Функции подразделений, сотрудника, ответственного за организацию обработки персональных данных.	10
15. Контрольные процедуры.....	14
16. Права Подразделений.....	14
17. Ответственность за нарушения выполнения требования настоящего документа.....	15
Приложение №1 "Информация по местам хранения персональных данных, обрабатываемых в подразделении"	16

1. Общие положения.

- 1.1. Настоящий документ определяет методы в отношении обработки персональных данных в ПАО СКБ Приморья «Примсоцбанк».
- 1.2. Действие настоящего документа распространяется на все структурные подразделения ПАО СКБ Приморья «Примсоцбанк».
- 1.3. Требования по обеспечению безопасности персональных данных для сотрудников ПАО СКБ Приморья «Примсоцбанк» определяются отдельным нормативным документом (разделом документа).
- 1.4. Персональные данные относятся к сведениям конфиденциального характера.
- 1.5. Правовым основанием для обработки персональных данных в ПАО СКБ Приморья «Примсоцбанк» является Законодательство РФ, в том числе Федеральный закон от 27.07.2006г. № 152-ФЗ «О персональных данных», ст. 86-90 Трудового кодекса Российской Федерации, Лицензия Банка России №2733 на осуществление банковских операций, Устав ПАО СКБ Приморья «Примсоцбанк» с последующими изменениями и дополнениями.
- 1.6. Целью обработки персональных данных является: осуществление банковских операций и иной деятельности, предусмотренной Уставом ПАО СКБ Приморья «Примсоцбанк», а также осуществление трудовых отношений с работниками ПАО СКБ Приморья «Примсоцбанк» и физическими лицами, намеревающимися вступить в трудовые отношения с ПАО СКБ Приморья «Примсоцбанк».
- 1.7. Под категорию персональных данных подпадает:
 - фамилия, имя, отчество;
 - год, месяц, дата рождения;
 - место рождения;
 - гражданство;
 - адрес;
 - ИНН;
 - телефон, факс;
 - электронная почта;
 - паспортные данные, данные документа, удостоверяющего личность;
 - страховой номер индивидуального лицевого счета (СНИЛС);
 - образование;
 - профессия;
 - сведения о трудовой деятельности;
 - социальное положение;
 - имущественное положение;
 - доходы;
 - номер банковского счета;
 - номер договора;
 - полис страхования;
 - семейное положение;
 - состав семьи, сведения о близких родственниках;
 - сведения о воинской обязанности.
- 1.8. Категории субъектов, персональные данные которых обрабатываются: физические лица, состоящие в договорных отношениях с ПАО СКБ Приморья «Примсоцбанк», изъявившие желание вступить в договорные отношения с ПАО СКБ Приморья «Примсоцбанк», либо совершающие (желающие совершить)

банковские операции и сделки с ПАО СКБ Приморья «Примсоцбанк», работники ПАО СКБ Приморья «Примсоцбанк».

- 1.9. Обработка персональных данных осуществляется смешанным способом с передачей по внутренним сетям и сетям общего пользования с использованием криптографических средств защиты информации и включает в себя: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- 1.10. Дата начала обработки персональных данных: 04.03.1994 года.

2. Термины и определения.

- 2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).
- 2.2. Банк – ПАО СКБ Приморья «Примсоцбанк», организующий и осуществляющий обработку персональных данных, а также определяющий цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- 2.3. 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, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
- 2.4. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.
- 2.5. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- 2.6. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- 2.7. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных, или в результате которых невозможно восстановление информации с носителя.
- 2.8. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- 2.9. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- 2.10. Контролируемая зона - пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
- 2.11. Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. Сокращения.

ПЭВМ – персональная электронная вычислительная машина (компьютер).

4. Согласие на обработку персональных данных.

- 4.1. Субъект персональных данных самостоятельно принимает решение о даче согласия на обработку его персональных данных Банком.
- 4.2. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных.
- 4.3. Для каждой из категорий субъектов персональных данных, указанных в п. 1.8 настоящего документа разрабатывается и утверждается собственная форма согласия на обработку персональных данных.
- 4.4. В случае отказа субъекта персональных данных предоставить согласие на обработку своих персональных данных, его обслуживание и заключение договоров становится невозможным, за исключением случаев:
 - исполнения и заключения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных;
 - заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

5. Сроки обработки персональных данных.

- 5.1. Сроки обработки персональных данных определяются в соответствии с:
 - сроками действия договоров с субъектами персональных данных;
 - иными требованиями законодательства и нормативных документов Банка России.

6. Поручение обработки персональных данных третьему лицу.

- 6.1. В случае, если Банк на основании согласия субъекта персональных данных и договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом режима конфиденциальности персональных данных и безопасности персональных данных при их обработке.

7. Трансграничная передача персональных данных.

- 7.1. Банк в ходе своей деятельности может осуществлять трансграничную передачу персональных данных на территорию иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных.

- 7.2. Трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, осуществляется в случаях:
- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
 - предусмотренных международными договорами Российской Федерации;
 - исполнения договора, стороной которого является субъект Персональных данных;
 - защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

8. Обеспечение безопасности персональных данных, обрабатываемых с использованием средств автоматизации.

- 8.1. Все информационные системы персональных данных размещаются на серверах Банка, которые размещены в контролируемой зоне, в помещении с ограниченным доступом. Перечень лиц, имеющих право доступа в данное помещение, определяется приказом Банка.
- 8.2. База данных информации содержащей персональные данные граждан Российской Федерации находится на территории Российской Федерации.
- 8.3. Все информационные системы персональных данных подлежат обследованию с целью определения требований к защите персональных данных для обеспечения необходимого уровня защищенности и нейтрализации актуальных угроз.

9. Обеспечение безопасности персональных данных, обрабатываемых без использования средств автоматизации.

- 9.1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
- 9.2. Под данный тип обработки персональных данных подпадают: обработка бумажных форм документов, электронных документов в виде файлов на ПЭВМ (как созданных вручную, так и «выгруженных» из информационных систем персональных данных), содержащих персональные данные.
- 9.3. Информация, содержащаяся в ПЭВМ, размещается в контролируемой зоне Банка, доступ в помещения ограничен в соответствии с «Инструкцией о порядке осуществления пропускного и внутри объектового режимов в ОАО СКБ Приморья «Примсоцбанк».
- 9.4. Информация, содержащаяся в ПЭВМ на торговых площадках (супермаркетов, магазинов, др. точках продаж) в обязательном порядке зашифровывается.
- 9.5. Доступ к информации на ПЭВМ осуществляется при предъявлении персонального идентификатора (логина) и пароля.

9.6. Отдельным распорядительным документом утверждается перечень мест хранения персональных данных с указанием категорий персональных данных и наименования подразделения, сотрудники которых имеют доступ к персональным данным.

10. Организация и управление доступом к персональным данным.

10.1. Все информационные системы персональных данных являются также информационными активами Банка. Доступ к информационным системам персональных данных, равно как и доступ к персональным данным, обрабатываемых в этих системах, блокировка и подтверждение доступа осуществляется в соответствии с регламентом процесса «Порядок доступа к информационным активам ПАО СКБ Приморья «Примсоцбанк». Решение о предоставлении доступа принимает руководитель сотрудника и руководитель подразделения Банка - владельца информационного актива.

10.2. Разрешение на доступ к бумажным документам, содержащим персональные данные, осуществляется в виде резолюции на документе.

10.3. Сотрудники Банка могут получать разрешение на доступ к персональным данным в соответствии со следующей схемой:

Кто выдает Разрешение	К каким сведениям	Кому
Председатель Правления Банка и Первый заместитель Председателя Правления	К персональным данным любых категорий	Сотрудникам Банка, представителям сторонних организаций
Заместители Председателя Правления, Исполнительный директор.	К персональным данным любых категорий в пределах своей компетенции	Сотрудникам Банка, представителям сторонних организаций
Главный бухгалтер, его заместители	К персональным данным, обрабатываемым в любом подразделении	Сотрудникам любых подразделений
Начальники Управлений, их заместители	К персональным данным, обрабатываемым Управлением	Сотрудникам Управлений Банка, сотрудникам Банка - соисполнителям работ
Начальники отделов	К персональным данным, обрабатываемым отделом	Сотрудникам отделов Банка, сотрудникам своего Управления - соисполнителям работ
Начальники самостоятельных отделов	К персональным данным, обрабатываемым отделом	Сотрудникам своих отделов, сотрудникам Банка – соисполнителям работ
В филиалах, дополнительных офисах, операционных офисах: Руководители, главные бухгалтера и их заместители	К персональным данным, обрабатываемым филиалом (дополнительным офисом, операционным офисом)	Работникам своих филиалов (дополнительных офисов, операционных офисов) Банка, представителям сторонних организаций

10.4. Доступ к информационным системам персональных данных осуществляется через экранные формы автоматизированных систем.

11. Обработка обращений и запросов.

11.1. Банк обязан, по запросу субъекта персональных данных предоставить информацию, 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 место нахождения 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, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом №152-ФЗ «О персональных данных»;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом №152-ФЗ «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 законодательством РФ.

11.2. Банк имеет право отказать в предоставлении информации о персональных данных субъекту персональных данных (ограничить объем предоставляемой информации) в соответствии с законодательством РФ, в том числе если:

- обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

11.3. 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.

11.4. Информация предоставляется субъекту персональных данных или его представителю Банком при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать:

- номер основного документа, удостоверяющего личность субъекта персональных данных или 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 или его представителя.

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

- 11.5. Срок предоставления информации по запросу составляет не более тридцати дней с даты его получения.
- 11.6. При отказе в предоставлении информации по запросу или при обращении субъекта персональных данных или его представителя, Банк предоставляет в письменной форме мотивированный ответ в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.
- 11.7. 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 обязан внести 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 обязан уничтожить такие персональные данные. Банк обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях и принятых мерах, а также принять меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.
- 11.8. Срок предоставления необходимой информации по запросу уполномоченного органа по защите прав субъектов персональных данных составляет не более тридцати дней с даты получения такого запроса.

12. Хранение персональных данных.

- 12.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем это 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. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.
- 12.2. Способ хранения материальных носителей персональных данных должен исключать несанкционированный доступ к ним:
 - 12.2.1. Рабочее место сотрудника должно быть организовано таким образом, чтобы исключалось обозрение находящихся на столе документов, содержащих персональные данные лицами, не имеющими к ним отношения.
 - 12.2.2. При выходе из помещения всех сотрудников оно должно быть закрыто на ключ.
 - 12.2.3. Доступ к документам в помещении санкционирован только сотрудникам, имеющим право входа в данное помещение. Присутствие в помещении других сотрудников возможен только под контролем сотрудника(-ов) имеющего право входа в помещение. Санкцию на доступ к документам в помещении сотрудникам, не имеющим право входа в помещение, предоставляется руководителем подразделения, за которым закреплено данное помещение.

13. Уничтожение персональных данных.

- 13.1. Банк прекращает обработку персональных данных и уничтожает собранные персональные данные, если иное не установлено законодательством РФ, в сроки, установленные законодательством РФ в следующих случаях:

- 13.1.1. По достижении целей обработки или утрате необходимости в ее достижении.
- 13.1.2. По требованию субъекта персональных данных или Уполномоченного органа по защите прав субъекта персональных данных – если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленных целей обработки.
- 13.1.3. При невозможности устранения Банком допущенных нарушений при обработке персональных данных.
- 13.2. Уничтожение или обезличивание персональных данных, если это допускается материальным носителем, выполняется способом, исключающим дальнейшую обработку персональных данных (при необходимости - с сохранением возможности обработки иных данных, зафиксированных на данном материальном носителе).
- 13.3. Уничтожение персональных данных на носителях персональных данных с последующим выносом носителей за пределы контролируемой зоны, должно выполняться одним из следующих способов:
 - 13.3.1. Бумажный носитель персональных данных уничтожается путем измельчения на бумагорезательной машине, сжигания, иным способом, исключающим возможность восстановления информации.
 - 13.3.2. Уничтожение персональных данных на дискетах, flash-носителях, картах памяти, жестких дисках осуществляется согласно алгоритму в соответствии с ГОСТ Р50739-95, либо путем физического разрушения носителя (микросхем, пластин диска).

14. Функции подразделений, сотрудника, ответственного за организацию обработки персональных данных.

- 14.1. Функции сотрудника, ответственного за организацию обработки персональных данных.
 - 14.1.1. Организация работ по исполнению резолюций Руководства Банка, выдача поручений и контроль их выполнения, назначение и контроль работ исполнителей, сбор необходимых документов, согласование и визирование ответов на запросы, полученных от субъектов персональных данных или от Уполномоченных надзорных органов относительно обработки персональных данных.
 - 14.1.2. Организация работ по созданию специальной комиссии и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области обработки персональных данных.
 - 14.1.3. Организация и проведение работ по обучению (повышению осведомленности) работников в области защиты персональных данных.
 - 14.1.4. Проверка уровня осведомленности работников в области защиты персональных данных.
- 14.2. Функции Отдела информационной безопасности управления оценки банковских рисков.
 - 14.2.1. Организация процедуры обследования информационных систем персональных данных и мониторинг событий в области защиты персональных данных.
 - 14.2.2. Организация подготовки и направление в уполномоченный орган по защите прав субъектов персональных данных «Уведомления об обработке персональных

данных», а в случае изменения сведений, содержащихся в Реестре Банков, осуществляющих обработку персональных данных — направление сведений о таких изменениях.

- 14.2.3. Организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию угроз безопасности с использованием требований по обеспечению безопасности персональных данных.
- 14.2.4. Разработка предложений по совершенствованию системы защиты персональных данных.
- 14.2.5. Подготовка материалов для проведения мероприятий по повышению осведомленности работников Банка по вопросам обеспечения безопасности персональных данных.
- 14.2.6. Участие в проведении работ по вводу в эксплуатацию (монтаж, настройка и проверка работоспособности) средств защиты информации в соответствии с эксплуатационной и технической документацией.

14.3. Функции Управления по персоналу и организационному развитию.

- 14.3.1. Обеспечение соответствия обработки персональных данных работников Банка (лиц желающих вступить в трудовые отношения) требованиям законодательства в области обработки персональных данных, в частности, требованиям Трудового Кодекса Российской Федерации.
- 14.3.2. Анализ и оценка соответствия внутренних нормативных документов Банка, в части касающейся обработки персональных данных работников Банка (лиц желающих вступить в трудовые отношения), а в случае выявления несоответствий — внесение необходимых изменений, в том числе в должностные инструкции работников.
- 14.3.3. Организация работ по ознакомлению работников Банка, под роспись, с «Положением об обработке персональных данных в ПАО СКБ Приморья «Примсоцбанк».

14.4. Функции Юридического управления.

- 14.4.1. Анализ законодательства Российской Федерации в области обработки персональных данных.
- 14.4.2. Анализ и оценка соответствия типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, требованиям законодательства Российской Федерации в области обработки персональных данных, а в случае выявления несоответствий - выработка рекомендаций по их устранению.
- 14.4.3. Анализ и оценка соответствия договорной базы Банка требованиям законодательства Российской Федерации в области обработки персональных данных, а в случае выявления несоответствий — внесение соответствующих изменений (дополнений).
- 14.4.4. Подготовка правовых заключений и консультационная работа, включающая консультирование работников Банка по вопросам, связанным с исполнением и применением требований настоящего положения и законодательства Российской Федерации в области обработки персональных данных.

14.5. Функции Управления автоматизации.

- 14.5.1. Эксплуатация информационных систем персональных данных в соответствии с организационно-технической и эксплуатационной документацией.
- 14.5.2. Организация мероприятий по восстановлению персональных данных, в том числе модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- 14.5.3. Установка и ввод в эксплуатацию (проведение работ совместно с отделом информационной безопасности, связанных с монтажом, настройкой и проверкой работоспособности) средств защиты информации в соответствии с эксплуатационной и технической документацией.
- 14.5.4. Реализация предложений по совершенствованию системы защиты персональных данных.

14.6. Функции Службы внутреннего контроля (комплаенс службы).

- 14.6.1. Контроль соответствия принимаемых в банке внутренних документов требованиям законодательства РФ в области защиты персональных данных, мониторинг мероприятий, связанных с регуляторным риском в области защиты персональных данных.

14.7. Функции Службы внутреннего аудита.

- 14.7.1. Проведение плановой проверки соблюдения подразделениями Банка требований внутренних документов Банка в области защиты персональных данных.

14.8. Функции отдела банковского надзора.

- 14.8.1. Организация работ по размещению оборудования информационных систем персональных данных, в части выполнения требований по сохранности носителей персональных данных и средств защиты информации, а также исключения возможности проникновения и неконтролируемого пребывания посторонних лиц.
- 14.8.2. Организация и проведение работ по обеспечению безопасности помещений, в которых производится обработка персональных данных, а также находятся на хранении материальные носители персональных данных, в том числе выработка мер, необходимых для обеспечения таких условий.

14.9. Служба качества обслуживания клиентов.

- 14.9.1. Прием обращений, запросов от субъектов персональных данных, подготовка, согласование ответов с юридическим управлением, сотрудником, ответственным за организацию обработки персональных данных, и другими заинтересованными подразделениями.

14.10. Функции руководителей всех подразделений.

- 14.10.1. Организация проведения первичных инструктажей сотрудников по вопросам обеспечения безопасности персональных данных.

14.10.2. Предоставляют сотруднику, ответственному за организацию обработки персональных данных Банка заполненное Приложение №1 при изменении информации по местам хранения персональных данных либо по отдельному распоряжению.

15. Контрольные процедуры.

15.1. Ответственность за ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных осуществляется:

- Управлением по персоналу и организационному развитию при первичном оформлении сотрудника, при этом работник подписывает обязательство о неразглашении персональных данных работников.
- Администраторами информационной безопасности – при оформлении доступа к информационным активам, при этом работник подписывает «Лист прохождения обучения сотрудников ПАО СКБ Приморья «Примсоцбанк» по вопросам информационной безопасности», в котором отражены изученные сотрудником вопросы.

15.2. Контроль исполнения процедуры, указанной в п.15.1 выполняется при согласовании доступов к информационным активам:

- отделом информационной безопасности – в Головном офисе;
- непосредственным руководителем – в филиалах и дополнительных офисах.

15.3. Контроль отсутствия проникновения и неконтролируемого пребывания посторонних лиц в Банке осуществляется охранным агентством (либо охранниками из штата Банка) на постоянной основе.

15.4. Контроль уровня осведомленности персонала выполняется путем организации управлением по персоналу и организационному развитию тестирования не реже 1 раза в два года.

15.5. Контроль доступа к информационным активам (содержащих персональные данные) выполняется отделом информационной безопасности при рассмотрении заявок на доступ и выполняется на постоянной основе.

15.6. Контроль соблюдения требований по обеспечению информационной безопасности персональных данных выполняется отделом информационной безопасности на постоянной основе.

16. Права Подразделений.

Подразделения, осуществляющие функции по организации защиты персональных данных, имеют право на:

16.1. Запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных в Банке.

16.2. Привлечение к проведению работ по защите персональных данных других подразделений Банка.

16.3. Привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций.

16.4. Контроль деятельности структурных подразделений Банка, в части выполнения ими требований по обеспечению безопасности персональных данных.

17. Ответственность за нарушения выполнения требования настоящего документа.

17.1. Сотрудники, осуществляющие непосредственную обработку персональных данных несут персональную ответственность за сохранение и обеспечение конфиденциальности информации.

17.2. Лица, виновные в нарушении требований настоящего Положения, несут предусмотренную законодательством Российской Федерации ответственность.

Информация по местам хранения персональных данных, обрабатываемых в подразделении.

Наименование подразделения: _____

Номер помещения: _____

№	Категория персональных данных	Признак хранения: Хранится: «Да» Иначе «Нет»	Категория субъектов ¹ : 1- клиент (контрагент) 2- потенциальный клиент (контрагент) 3- сотрудник 4- лицо, устраивающееся на работу в банк	В каком виде ¹ : 1-Бумажный носитель, 2-Файл на персональном компьютере
1	фамилия, имя, отчество			
2	год рождения			
3	месяц рождения			
4	дата рождения			
5	место рождения			
6	гражданство			
7	адрес			
8	ИНН			
9	телефон, факс			
10	электронная почта			
11	паспортные данные, данные документа, удостоверяющего личность			
12	страховой номер индивидуального лицевого счета (СНИЛС)			
13	образование			
14	профессия			
15	сведения о трудовой деятельности			
16	социальное положение			
17	имущественное положение			
18	доходы			
19	номер банковского счета			
20	номер договора			
21	полис страхования			
22	семейное положение			
23	состав семьи, сведения о близких родственниках			
24	сведения о воинской обязанности			

Заполняются только незатемненные ячейки таблицы.

Руководитель структурного подразделения _____

Роспись

ФИО

« _____ » _____ 20__ г.

¹При выборе одновременно нескольких вариантов, необходимо указывать информацию через запятую.