«УТВЕРЖДАЮ» Председатель
Правления
ООО «Камский коммерческий банк»
_____ Габдуллина Р.М.

Положение о порядке обработки персональных данных ООО «Камский коммерческий банк» Версия 1.0.270815

Начальник УАВБУиА		/ Дьяконов А.А. /	27.08.2015г
(должность)	(подпись)	(Ф.И.О.)	(дата)
СОГЛАСОВАНО:			
Зам. начальник УАВБУиА		/ Марыняк Э.Я. /	27.08.2015г.
(должность)	(подпись)	(Ф.И.О.)	(дата)
Начальник ИБ		/ Хураскин С.М. /	27.08.2015.
(должность)	(подпись)	(Ф.И.О.)	(дата)
Зам. Председателя Правления		/ Габдрахманова З.С./	
(должность)	(подпись)	(Ф.И.О.)	(дата)
Зам. Председателя Правления		/ Хабибуллина Э.И./	27.08.15
(должность)	(подпись)	(Ф.И.О.)	(дата)

Набережные Челны, 2015 г

1 НАЗНАЧЕНИЕ

Настоящее Положение о порядке обработки персональных данных (далее – Положение) предназначено для применения при организации и исполнении процессов обработки ПДн в Банке в соответствии с требованиями Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014), а также требованиями нормативных документов РФ в области обработки и защиты ПДн.

2 ОБЛАСТЬ ПРИМЕНЕНИЯ

Требования настоящего Положения распространяются на подразделения и должностные лица Банка, принимающие участие в процессах обработки ПДн.

3 ОТВЕТСТВЕННОСТЬ

Владелец процесса: ответственный за организацию обработки персональных данных в Банке и осуществление контроля соблюдения требований Закона 152-ФЗ «О персональных данных».
Актуализация: Настоящее Положение пересматривается не реже 1 раза в год или в следующих случаях:

- изменение требований законодательства РФ в области обработки ПДн, а также требований комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС[1];
- изменение основных направлений Политики информационной безопасности Банка;
- изменение организационной и технологической инфраструктуры, в рамках которых обрабатываются ПДн;
- выявление снижения общего уровня ИБ при выполнении банковского информационного технологического процесса, в рамках которого обрабатываются персональные данные (по результатам регулярного мониторинга или аудита).

Актуализация проводится ответственным за организацию обработки персональных данных в Банке и осуществление контроля соблюдения требований Закона 152-ФЗ «О персональных данных».
Ответственность за исполнение: Все сотрудники Банка, принимающие участие в процессах обработки ПДн, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Положением, в пределах, определенных действующим законодательством РФ.

Руководитель, разрешающий доступ работника к конфиденциальному документу, содержащему персональные данные, несет персональную ответственность за данное разрешение.

За несоблюдение требований настоящего Положения законодательством РФ в области ПДн предусмотрена дисциплинарная, административная, гражданская и уголовная ответственность, а так же дисциплинарные взыскания в соответствии с Трудовым кодексом РФ.

4 СРОК ДЕЙСТВИЯ ДОКУМЕНТА, КОНТРОЛЬ ИСПОЛНЕНИЯ, ЗАМЕНЯЕМЫЕ ДОКУМЕНТЫ

Вступает в силу: со дня утверждения.
Контроль исполнения: Отдел информационной безопасности.

5 ТЕРМИНЫ, СОКРАЩЕНИЯ, УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Банк – «Камский коммерческий банк» (ООО).
Автоматизированная обработка персональных данных – Обработка персональных данных с помощью средств вычислительной техники.
Безопасность персональных данных – Состояние защищенности ПДн от неправомерных действий, характеризуемое способностью пользователей, технических средств и информационных систем обеспечить конфиденциальность, целостность и доступность ПДн при их обработке, независимо от формы их представления.
Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

---

[1] Сведения о внесении изменений в комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС в части касающейся обработки персональных данных доводятся до владельца процесса Отделом информационной безопасности.

Вирус (компьютерный, программный) – Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.
Внутренняя типовая форма – Документ, состав данных и порядок обработки которого не установлен законодательством РФ, и использующийся во внутренних бизнес-процессах Банка.
Доступ к информации – Возможность получения информации и ее использования.
Защита информации – Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
Защита информации от утечки – Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней.
Защищаемая информация – Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.
ИБ – информационная безопасность.
Информационная система персональных данных – Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
Информационные технологии – Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.
Информация – Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.
Конфиденциальная информация – Информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.
Накопление персональных данных – Деятельность, следствием которой является увеличение объема обрабатываемых персональных данных.
Несанкционированный доступ (несанкционированные действия) – Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.
Обезличивание персональных данных – Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
Обработка персональных данных – Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
Общедоступные источники персональных данных – Источники персональных данных, создаваемые в целях информационного обеспечения (в том числе справочники, адресные книги).
Оператор персональных данных (оператор) – Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
Персональные данные – ПДн, любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
Пользователь персональных данных – Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты такой обработки.
Предоставление персональных данных – Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
Процесс обработки персональных данных – Бизнес-процесс Банка, в рамках которого осуществляется обработка персональных данных.
Распространение персональных данных – Действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
СЗПДн – система защиты персональных данных.
Средство вычислительной техники – Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.
Структурное подразделение – подразделение (от уровня отдела и выше), входящее в состав «Камский коммерческий банк» (ООО) в соответствии с организационно-штатной структурой.
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.
Целостность информации – Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Электронный документ – Документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.
Электронная подпись – Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

6 ОБЩИЕ ПОЛОЖЕНИЯ

6.1. Настоящее Положение устанавливает требования к сбору, хранению, передаче, использованию, уничтожению и любым другим видам обработки ПДн, принятым в Банке.
6.2. Все работники Банка ознакамливаются с данным Положением и изменениями к нему.
6.3. Обработка ПДн осуществляется на законной и справедливой основе.
6.4. Обработка ПДн ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн.
6.5. не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.
6.6. Обработке подлежат только ПДн, которые отвечают целям их обработки.
6.7. Содержание и объем обрабатываемых ПДн соответствуют заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.
6.8. При обработке ПДн обеспечивается точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн. Оператор принимает необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
6.9. Хранение ПДн осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7 ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии с принципами обработки ПДн, указанными в п. 6 Положения, в Банке определены состав и цели обработки ПДн, требования к обработке ПДн, а также методы и способы обработки ПДн.

7.1. Состав и цели обработки персональных данных

В Банке определен перечень обрабатываемых ПДн с указанием целей и правовых оснований для обработки каждой из категорий ПДн, а также для каждой цели определены:
- объем и содержание персональных данных;
- сроки обработки, в том числе сроки хранения персональных данных;
- необходимость получения согласия субъектов персональных данных.

Перечень приводится в документе «Перечень обрабатываемых ПДн».

В Банке обрабатываются ПДн следующих категорий субъектов ПДн в соответствующих целях:

- **Персональные данные работников** – в целях обеспечения соответствия требованиям Трудового кодекса и других нормативно-правовых актов РФ, а также ведения учета в кадровом делопроизводстве.
- **Персональные данные соискателей на вакантные должности** – в целях рассмотрения резюме и отбора кандидатов на вакантную должность для дальнейшего трудоустройства в Банк.
- **Персональные данные клиентов** – физических лиц – в целях оказания услуг в рамках основной деятельности и исполнения требований законодательства РФ. Данные могут обрабатываться также в маркетинговых целях.
- **Персональные данные потенциальных клиентов** - обрабатываемых в целях принятия решения о предоставлении услуги. Данные могут обрабатываться также в маркетинговых целях.
- **Персональные данные посетителей** – в целях принятия решения о допуске на территорию Банка и последующего контроля.
- **Персональные данные представителей клиентов** – юридических и физических лиц – в целях оказания услуг в рамках основной деятельности и исполнения требований законодательства РФ.
- **Персональные данные выгодоприобретателей** – физических лиц – в целях исполнения требований законодательства РФ.

- **Персональные данные контрагентов клиента** – в целях исполнения требований законодательства РФ.
- **Персональные данные физических лиц, в отношении которых имеются сведения об их участии в экстремистской деятельности либо сведения о недействительности их паспортов (полученные от Федеральнйо миграционной службы)** – в целях исполнения требований законодательства РФ.
- **Персональные данные представителей контрагентов** – юридических лиц – в целях оказания услуг в рамках хозяйственной деятельности.
- **Персональные данные контрагентов физических лиц** – в целях оказания услуг в рамках хозяйственной деятельности.
- **Персональные данные о состоянии здоровья** – в Банке допускается обработка специальной категории ПДн, касающейся состояния здоровья субъекта ПДн, только в следующих случаях:
  - обработка необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта ПДн невозможно;
  - обработка осуществляется в рамках предоставления субъектам ПДн услуг по медицинскому страхованию (Банк выступает в роли страхователя или агента страховщика) либо другим видам страхования, при которых обработка ПДн о состоянии здоровья является необходимым условием оказания услуги.

  Обработка ПДн о здоровье допускается только без использования средств автоматизации.

  Банк прекращает обработку ПДн о здоровье, если устранены причины, вследствие которых они обрабатывались.

В Банке не допускается обработка ПДн следующих категорий:

- **Специальные категории ПДн** (ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, и интимной жизни).

7.2. ОБЩИЕ ТРЕБОВАНИЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В целях соблюдения положений комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» БР ИББС, а также действующих нормативных документов РФ при обработке ПДн в Банке установлены следующие обязательные требования:

- обработка ПДн осуществляется с соблюдением Конституции Российской Федерации и законов и иных нормативных правовых актов РФ в целях обеспечения личной безопасности субъекта ПДн и членов его семьи, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- персональные данные не могут быть использованы в целях причинения имущественного и/или морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации;
- работники ознакамливаются под подпись с документами Банка, устанавливающими порядок обработки их ПДн, а также с правами и обязанностями в этой области в соответствии с действующими нормативными документами;
- обработка ПДн не допускается без письменного согласия субъекта ПДн, за исключением случаев, установленных федеральным законом.

7.3. МЕТОДЫ И СПОСОБЫ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В процессах обработки ПДн в Банке применяются следующие методы:

- автоматизированная обработка;
- неавтоматизированная обработка (без использования средств автоматизации);
- смешанная обработка.

В ходе своей деятельности Банк получает и осуществляет передачу ПДн третьим лицам в целях заключения договоров с субъектом ПДн, исполнения договорных обязательств, а также в иных целях, определенных в согласии субъекта персональных данных на обработку ПДн.

Банк строго определяет круг лиц, допущенных к ПДн. Банк не обнародует персональные данные в средствах массовой информации, и не размещает в информационно-телекоммуникационных сетях.

Доступ третьих сторон к ПДн допускается только с письменного согласия субъекта или без такового в случаях, если такой доступ разрешен действующим законодательством РФ, либо если доступ предоставляется к общедоступным ПДн.

Банк получает и передает ПДн в целях исполнения договорных обязательств, а также поручает обрабатывать персональные данные третьей стороне на основании договоров.

Существенным условием договоров является обязанность обеспечения сторонами соблюдения конфиденциальности и обеспечение безопасности ПДн при их обработке, а также должны быть указаны требования к защите обрабатываемых ПДн в соответствии с законодательством, определен перечень действий (операций) с ПДн, которые будут совершаться.

Обеспечение безопасности персональных данных, согласно договорам, третьей стороной достигается путем соблюдения следующих мер:

1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

5) учетом машинных носителей персональных данных;

6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) контролем принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

В договорах в обязательном порядке определяются цели обработки ПДн и порядок обмена информацией. Банком передаются ПДн только в объеме необходимом для достижения заявленных целей обработки.

Ответственность за соблюдение условий договоров о передаче ПДн в части обеспечения конфиденциальности и безопасности при обработке ПДн, а также контроля над исполнением этих условий принимающей стороной.

7.3.1. Сбор персональных данных

Банк получает ПДн из следующих источников:

- непосредственно от субъекта ПДн;
- от третьей стороны, в целях исполнения договорных обязательств, заключения договоров или исполнения требований нормативных документов РФ, при условии предоставления оператору подтверждения наличия оснований;
- от другого субъекта ПДн, в целях реализации его законных прав.

При получении ПДн не от самого субъекта ПДн, Банк предоставляет субъекту ПДн до начала обработки следующую информацию:

- адрес и наименование Банка;
- цели и правовые основания обработки ПДн;

- предполагаемые пользователи ПДн;
- права субъекта ПДн;
- источник получения персональных данных.

Банк освобождается от обязанности предоставить субъекту ПДн указанные выше сведения, в случаях, если:

- субъект ПДн уведомлен об осуществлении обработки его персональных данных соответствующим оператором, были получены ПДн;
- ПДн получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого, либо выгодоприобретателем или поручителем по которому является субъект ПДн;
- ПДн сделаны общедоступными субъектом ПДн или получены из общедоступного источника;
- оператор осуществляет обработку ПДн для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта ПДн;
- предоставление субъекту ПДн сведений нарушает права и законные интересы третьих лиц.

При получении ПДн родственников от работника (страхование работников), ответственность за уведомление родственников о факте передачи их ПДн возлагается на самого работника.

7.3.2. Накопление персональных данных

Накопление ПДн происходит в результате деятельности Банка. Банк накапливает ПДн следующими путями:

- сохранение копий документов;
- внесение сведений в учетные формы (на бумажные носители и в базы данных автоматизированных систем);
- получение оригиналов документов (трудовая книжка, личный листок по учету кадров, автобиография и пр.).

7.3.3. Хранение персональных данных

Хранение ПДн в Банке осуществляется в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели их обработки и требования нормативных документов РФ, связанных с хранением документов, после чего данные могут быть обезличены (при необходимости).

Сроки хранения ПДн в Банке определены в документе «Перечень обрабатываемых ПДн».

Банк осуществляет хранение ПДн следующими способами:

- на машинных носителях, при автоматизированной обработке ПДн;
- на бумажных носителях, при обработке без использования средств автоматизации.

7.3.4. Предоставление персональных данных (взаимодействие с третьими сторонами)

При предоставлении ПДн субъекта Банк обязан соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных законодательством Российской Федерации;
- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные субъекта, обязаны соблюдать требования конфиденциальности;
- не сообщать ПДн работника в коммерческих целях без его письменного согласия;
- персональные данные субъекта могут быть предоставлены родственникам или членам семьи субъекта ПДн по письменному разрешению самого субъекта ПДн;
- не допускается отвечать на вопросы, связанные с предоставлением персональной информации по телефону, лицам, не подтвердившим свое право на получение данной информации (не знающим кодового слова и т.п.).

Банк в целях выполнения требований нормативных документов РФ и выполнения условий договорных отношений предоставляет ПДн следующим третьим сторонам:

- Налоговая служба РФ – в целях выполнения требований налогового законодательства, отправки отчетности по работникам и клиентам Банка. Предоставляются паспортные данные, финансовая информация (сумма начислений за расчетный период по форме № 2-НДФЛ).
- Федеральная служба по финансовым рынкам – в целях выполнения требований законодательства. Передаются: ФИО, данные документа, удостоверяющего личность, дата и место рождения, гражданство, данные миграционной карты, документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в РФ, данные о месте жительства (регистрации) и месте пребывания, ИНН (при наличии), контактная информация, сведения об операциях/сделках, о банковских счетах.
- Финансовая служба по финансовому мониторингу - в целях выполнения требований законодательства. Передаются: ФИО, данные документа, удостоверяющего личность, дата и место рождения, гражданство, данные миграционной карты, документа, подтверждающего право иностранного гражданина или лица без гражданства на пребывание (проживание) в РФ, данные о месте жительства (регистрации) и месте пребывания, ИНН (при наличии), контактная информация, сведения об операциях/сделках, о банковских счетах.
- Пенсионный фонд РФ – в целях выполнения требований пенсионного законодательства, отправки отчетности по работникам Банка. Предоставляются паспортные данные, данные о месте жительства, финансовая информация (сумма начислений за расчетный период, сумма удержанных пенсионных взносов).
- Страховые организации – в целях получения услуг по страхованию работников Банка. Предоставляются паспортные данные, данные о месте жительства.
- Кредитные организации – в целях открытия расчетного счета, оформление банковских карт, перевод денежных средств. Предоставляются паспортные данные, данные о месте жительства, контактная информация, сведения об операциях, сведения об ИНН клиента.
- Центральный банк РФ – в целях выполнения банковских операций. Предоставляются паспортные данные, данные о месте жительства, контактная информация, сведения об операциях, сведения об ИНН клиента.
- Организации-грузоперевозчику – в целях получения курьерских услуг Банком. Предоставляются сведения об отправлении, контактная информация, данные о месте жительства.
- Бюро кредитных историй – в целях получения услуг по формированию, обработке и хранению кредитных историй клиентов Банка. Предоставляется информация о кредитной истории клиента – сумма кредита, процентная ставка, дата выдачи и погашения, наличие просрочки и т. д.
- "Партнеры Банка - в целях и в объеме, определенном в согласии субъекта персональных данных на обработку ПДн.
- Предоставление ПДн правоохранительным и судебным органам с целью исполнения запросов, полученных от правоохранительных и судебных органов по находящихся в их производстве делам;
- Иным третьим лицам в случаях, предусмотренных законодательством Российской Федерации или договором.

7.3.5. Обезличивание персональных данных

В Банке может использоваться обезличивание ПДн в тех процессах, где данную меру возможно осуществить. Обезличивание ПДн организовано таким способом, чтобы не влиять негативным образом на существующие в Банке процессы обработки ПДн.

Обезличивание ПДн освобождает Банк от обеспечения конфиденциальности этих ПДн и сбора дополнительных согласий с субъектов ПДн при совершении различных операций с ПДн.

7.3.6. Блокирование персональных данных

В случае выявления неправомерной обработки ПДн или неточных ПДн при обращении (запросе) субъекта ПДн, либо уполномоченного органа по защите прав субъектов ПДн Банк обязан осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту, или обеспечить их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц. Блокирование осуществляется также в случае отсутствия возможности уничтожения ПДн в течение срока, указанного в частях 3 и 5 статьи 21 ФЗ «О персональных данных».

7.3.7. Уничтожение ПДн

Банк уничтожает персональные данные в случае:

- достижения целей обработки ПДн или утраты необходимости в их достижении;
- получения требования субъекта ПДн – если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыва субъектом ПДн согласия на обработку своих ПДн (если отзыв согласия влечет за собой уничтожение ПДн;
- получения требования от уполномоченного органа по защите прав субъектов ПДн;
- невозможности устранения Банком допущенных нарушений при обработке ПДн.

Документы, содержащие персональные данные, подлежат хранению в порядке, предусмотренном комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»[2] БР ИББС и нормативными документами РФ, регламентирующими процесс обработки и обеспечения безопасности ПДн. Уничтожение персональных данных производится в соответствии с внутренними регламентирующими документами Банка.

Банк может заключать договоры с третьими сторонами на оказание услуг по уничтожению материальных носителей. При этом Банк и третья сторона соблюдают все правила для обеспечения конфиденциальности уничтожаемых данных.

Банк сообщает субъекту ПДн и (или) уполномоченному органу по защите прав субъектов об уничтожении соответствующих ПДн.

Не подлежат уничтожению ПДн клиентов Банка, подлежащие архивному хранению. Перечень таких ПДн ограничен и включает в себя следующие сведения:

- фамилия имя отчество;

- дата рождения;

- паспортные данные;

- индивидуальный номер налогоплательщика;

- свидетельство пенсионного страхования;

- и другие данные, хранение которых предусмотрено действующим законодательством

ПДн, подлежащие архивному хранению, не могут использоваться в целях информирования клиентов (sms рассылка, исходящие телефонные звонки, почтовые уведомления), а также обрабатываться иным образом, включая, но, не ограничиваясь накоплением, и предоставлением ПДн третьим лицам.

7.4. ОСОБЕННОСТИ НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ (БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ)

Под обработкой ПДн, осуществляемой без использования средств автоматизации, понимается обработка ПДн, зафиксированных на бумажных носителях.

7.4.1. Особенности сбора персональных данных

В Банк поступают бумажные носители (документы), содержащие ПДн в виде копий документов, удостоверяющих личность, резюме, автобиографий, справок, анкет, договоров, протоколов и пр.

Банк также осуществляет периодический сбор ПДн путем анкетирования субъектов ПДн либо запросом дополнительных сведений о субъекте ПДн в рамках заявленных целей обработки ПДн, не противоречащих положениям действующих нормативных документов РФ в области обработки и защиты ПДн.

---

[2] Введен в действие Приказом по Банку

7.4.2. Особенности накопления персональных данных

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), выполняются следующие условия:

- в типовую форму или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) включаются сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, наименование и адрес Банка, фамилия, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых в Банке способов обработки ПДн;
- в типовую форму включается поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, при необходимости получения письменного согласия на обработку ПДн;
- типовая форма составляется таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;
- в типовой форме исключается объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.
- При ведении журналов (реестров, книг), содержащих ПДн, необходимые для однократного пропуска субъекта ПДн на территорию Банка или в иных аналогичных целях, соблюдаются следующие условия:
- необходимость ведения такого журнала (реестра, книги) оформляется приказом, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию Банка без подтверждения подлинности ПДн, сообщенных субъектом ПДн;
- копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;
- ПДн каждого субъекта могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Банка.

7.4.3. Особенности хранения персональных данных

В Банке обеспечено раздельное хранение ПДн при разных целях обработки и не допускается фиксации на одном бумажном носителе ПДн, цели обработки которых заведомо несовместимы. Для обработки каждой категории ПДн используется отдельный бумажный носитель.

7.4.4. Особенности использования и предоставления (распространения) персональных данных

При необходимости использования или предоставления (распространения) определенных ПДн отдельно от находящихся на том же бумажном носителе других ПДн осуществляется копирование ПДн, подлежащих предоставлению (распространению) или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих предоставлению (распространению) и использованию, и используется (предоставляется) копия ПДн.

7.5. ОСОБЕННОСТИ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Информационные системы ПДн, позволяющие осуществлять обработку ПДн с использованием средств автоматизации в Банке, выявлены, описаны и классифицированы.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

7.5.1. Особенности сбора и накопления персональных данных

Банк осуществляет дополнительное накопление ПДн, получаемых по электронной почте или из общедоступных электронных источников (интернет-сайты компаний – рекрутинговых агентств).

7.5.2. Особенности использования и распространения персональных данных

При необходимости использования или распространения определенных ПДн отдельно от находящихся на том же машинном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

Распространение и передача, в том числе и трансграничная передача ПДн при их обработке в информационных системах осуществляются Банком только по защищенным либо выделенным каналам связи. Банк передает по незащищенным каналам передачи только общедоступные ПДн.

7.5.3. Уничтожение записей, содержащих персональные данные, на машинных носителях

Уничтожение записей, содержащихся на машинных носителях, осуществляется способом, исключающим восстановление уничтоженных ПДн, в соответствии с Инструкцией по порядку учета, хранения и уничтожения носителей конфиденциальной информации[3].В случае принятия Банком положительного решения об уничтожении ПДн, (при поступлении соответствующего заявления от субъекта ПДн), производится уничтожение ПДн субъекта.

8 ОРГАНИЗАЦИЯ ДОСТУПА РАБОТНИКОВ К ПЕРСОНАЛЬНЫМ ДАННЫМ

Работники Банка получают доступ к ПДн исключительно в объеме, необходимом для выполнения ими конкретных трудовых (должностных) обязанностей.

Работник получает доступ к ПДн после:

- ознакомления и изучения требований настоящего Положения и иных организационно-распорядительных документов на систему защиты ПДн;
- прохождения обучения правилам обработки и обеспечения безопасности ПДн;
- ознакомления с видами ответственности за нарушение/невыполнение требований нормативных документов РФ в области обработки и защиты ПДн.

В случае обнаружения нарушений порядка предоставления прав доступа к персональным данным приостанавливается предоставление ПДн пользователям до выявления и устранения причин нарушений.

9 ВЗАИМОДЕЙСТВИЕ С ОРГАНАМИ ВЛАСТИ

В целях исполнения норм законодательства РФ, по мотивированному запросу органов власти Банк предоставляет запрашиваемую информацию о субъекте ПДн.

В Банке ответственность за взаимодействие с органами власти по вопросам обработки и защиты ПДн возлагается на Начальника отдела информационной безопасности (ответственного сотрудника, исполняющего роль согласно «Положению о ролях и ответственности за обработку и защиту персональных данных «Камский коммерческий банк» (ООО)»)[4]. При необходимости указанными лицами привлекаются работники подразделений, ответственные за защиту и обработку ПДн, в рамках их функциональных обязанностей.

9.1. ОРГАНЫ ВЛАСТИ, РЕГУЛИРУЮЩИЕ ОБЛАСТЬ ОБРАБОТКИ И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как уполномоченный орган по защите прав субъектов ПДн осуществляет федеральный государственный контроль (надзор) за соответствием обработки ПДн требованиям нормативных документов РФ в области обработки и защиты ПДн.

Контроль и надзор за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн, установленных Правительством Российской Федерации, может осуществляться Федеральной службой

---

[4] Утверждено Приказом по Банку

безопасности (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России), в пределах их полномочий и без права ознакомления с ПДн, обрабатываемыми в ИСПДн.

Роскомнадзор уполномочен проводить плановые и внеплановые проверки с целью осуществления контроля и надзора выполнения требований нормативных документов РФ в области обработки и защиты ПДн.

ФСТЭК России уполномочена проводить проверки с целью осуществления контроля и надзора выполнения требований законодательства Российской Федерации в области обеспечения защиты (не криптографическими методами) конфиденциальной информации, предотвращения ее утечки по техническим каналам, и за счет НСД к данной информации.

ФСБ России уполномочена проводить проверки с целью осуществления контроля и надзора за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности ПДн при их обработке в ИСПДн, в частности за выполнением требований использования шифровальных (криптографических) средств, применяемых для обеспечения безопасности ПДн.

Плановые проверки, проводятся на основании ежегодного плана проведения проверок, утвержденного руководителем Регулятора.

О проведении плановой проверки Банк уведомляется не позднее чем в течение трех рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Регулятора почтовым отправлением с уведомлением о вручении или иным доступным способом.

Основанием для проведения внеплановых проверок является:

- истечение срока исполнения Банком ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области ПДн;
- поступление обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о фактах возникновения угрозы причинения вреда жизни, здоровью граждан или фактах причинения вреда жизни, здоровью граждан.
- приказ руководителя Регулятора, изданный в соответствии с поручениями Президента Российской Федерации, Правительства Российской Федерации;
- нарушение прав и законных интересов граждан действиями (бездействием) Банком при обработке их ПДн;
- нарушение Банком требований законодательства Российской Федерации в области ПДн
- несоответствие сведений, содержащихся в уведомлении об обработке ПДн, фактической деятельности.

О проведении внеплановой выездной проверки Банк уведомляется не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом. Если в результате деятельности Банка причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление Банка о начале проведения внеплановой выездной проверки не требуется.

Основанием для проведения проверки Регулятором является приказ, утвержденный руководителем Регулятора. В приказе о проведении проверки указываются:

- наименование органа федерального государственного контроля (надзора);
- фамилии, имена, отчества должностных лиц, проводящих проверку;
- наименование (фамилия, имя, отчество) Оператора;
- цели, задачи, предмет проверки и срок ее проведения;
- правовые основания проведения проверки, в том числе подлежащие проверке обязательные требования законодательства Российской Федерации в области ПДн;
- сроки проведения и перечень мероприятий по контролю, необходимых для достижения целей и задач проведения проверки;
- перечень административных регламентов проведения мероприятий по контролю;
- перечень документов, представление которых Оператором необходимо для достижения целей и задач проведения проверки;
- даты начала и окончания проведения проверки.

Перед началом проверки должностное лицо Регулятора предъявляет Начальнику отдела Информационной Безопасности копию приказа о проведении проверки, заверенную гербовой печатью Регулятора, и служебное удостоверение.

На втором экземпляре копии приказа о проведении проверки, остающейся у должностного лица Регулятора, Начальник отдела Информационной Безопасности проставляет отметку о получении копии приказа о проведении проверки с указанием должности, фамилии, имени и отчества, а также даты и времени его получения.

Проверка может проводиться только должностными лицами Регулятора, которые указаны в приказе о ее проведении.

10 ПРАВА И ОБЯЗАННОСТИ СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Субъект ПДн имеет право на получение информации, касающейся обработки 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 место нахождения Банка, сведения о лицах (за исключением работников Банка), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту 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 федеральным законом;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу.

Указанные выше сведения предоставляются субъекту ПДн в доступной форме, и в них не содержатся ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

Банк в целях исполнения положений действующих нормативных документов РФ в области обработки и защиты ПДн, предоставляет указанные выше сведения субъекту ПДн или его законному представителю на основании соответствующего запроса.

Запрос субъекта ПДн сопровождается:

- предоставлением сведений о документе, удостоверяющим личность, с указанием сведений о дате выдачи указанного документа и выдавшем его органе и подпись субъекта ПДн или его законного представителя в случае непосредственного обращения субъекта ПДн с запросом;
- сведениями, подтверждающими 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;
- электронной подписью - в случае направления электронного запроса.

Кроме того, субъект ПДн имеет право:

- на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами;
- требовать разъяснения порядка принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения;
- заявить возражение против принятия решения на основании исключительно автоматизированной обработки ПДн;
- разъяснить порядок защиты своих прав и законных интересов.

Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.

11 ПРАВА И ОБЯЗАННОСТИ БАНКА

11.1. ПРАВА БАНКА

Банк имеет право:

- требовать от субъекта ПДн предоставления достоверных сведений о себе в порядке и объеме, предусмотренном законодательством Российской Федерации, а в случае их изменений своевременно уведомлять об этом Банк;
- отказать субъекту или его законному представителю, в предоставлении доступа к информации по формальным признакам в случае несоответствия содержания запроса требованиям, приведенным в разделе 10 настоящего Положения;
- отказать уполномоченному органу по защите прав субъектов в предоставлении доступа к информации по формальным признакам в случае несоответствия с порядком предоставления запросов от уполномоченного органа по защите прав субъектов, приведенным в разделе 9.1. настоящего Положения;
- осуществлять трансграничную передачу ПДн без дополнительного согласия субъекта ПДн в случае, если передаваемые ПДн являются общедоступными, или в случае обезличивания ПДн;
- поручать обработку ПДн третьим лицам на договорной основе.

Банк не имеет право:

- получать и обрабатывать ПДн субъекта ПДн о его политических, религиозных и иных убеждениях и частной жизни;
- получать и обрабатывать ПДн субъекта ПДн о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

11.2. ОБЯЗАННОСТИ БАНКА

Для защиты ПДн субъектов Банк обязан:

- обеспечить защиту ПДн субъекта от неправомерного их использования, утраты или искажения в порядке, установленном действующим законодательством;
- ознакомить работника с настоящим Положением и его правами в области защиты ПДн под расписку;
- осуществлять передачу ПДн субъекта только в соответствии с настоящим Положением и законодательством Российской Федерации;
- отказать уполномоченному органу по защите прав субъектов в предоставлении доступа к информации в случае несоответствия запроса требованиям действующего законодательства РФ;
- рассмотреть возражение субъекта ПДн и уведомить его о результатах рассмотрения такого возражения;
- разъяснить субъекту ПДн юридические последствия отказа в предоставлении своих персональных данных, если обязанность предоставления ПДн субъектом установлена федеральным законом (включая налоговое, трудовое право).

В случае выявления недостоверных ПДн или неправомерных действий с ними Банк обязан осуществить блокирование ПДн, относящихся к соответствующему субъекту, с момента получения такой информации на период проверки. В случае подтверждения факта недостоверности ПДн Банк на основании соответствующих документов обязан уточнить персональные данные и снять их блокирование.

Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 Федерального Закона «О персональных данных» № 152 от 27.07.2006.

В случае достижения цели обработки ПДн Банк обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

В случае отзыва субъектом ПДн согласия на обработку его ПДн Банк обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить персональные данные или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Банком и субъектом ПДн либо если Банк не вправе

осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение срока, указанного выше, Банк осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Банка) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

12 ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обеспечение информационной безопасности ПДн – это комплекс мер, направленный на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности ПДн и на обеспечение безопасности информации в процессе деятельности Банка.

Банк при обработке ПДн принимает необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в информационных системах ПДн, установленными комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» БР ИББС и нормативно-правовыми актами Российской Федерации, регламентирующими вопросы обеспечения информационной безопасности ПДн.

12.1. ОБЕСПЕЧЕНИЕ ВНУТРЕННЕЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Внутренняя защита ПДн включает следующие организационно-технические мероприятия:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работниками требований нормативно-методических документов по защите ПДн;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- защита паролями доступа персональных компьютеров, на которых содержатся персональные данные;
- ограничение доступа к сети Интернет с рабочих мест, имеющих доступ к ИСПДн;
- защита доступа к программным средствам ИСПДн паролями доступа;
- установка антивирусного программного обеспечения на рабочие станции и серверы;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находятся средства вычислительной техники ИСПДн либо хранятся документы, содержащие ПДн;
- соблюдение порядка уничтожения ПДн;
- своевременное выявление нарушений требований разрешительной системы доступа работниками подразделения;
- разъяснительная работа с работниками по предупреждению утраты ПДн, ценных сведений при работе с конфиденциальными документами.

12.2. ОБЕСПЕЧЕНИЕ ВНЕШНЕЙ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Внешняя защита включает следующие организационно-технические мероприятия:

- создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;
- посторонние лица (любое лицо, не имеющее непосредственного отношения к деятельности Банка, посетители, работники других организационных структур) не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в подразделениях, использующих персональные данные.

Для защиты ПДн соблюдается ряд мер организационно-технического характера:

- порядок приема, учета посетителей;

- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при интервьюировании и собеседованиях.

Конкретные мероприятия по защите ПДн с использованием или без использования рабочих станций определяются документом «Положение об обеспечении безопасности ПДн при обработке».

Защита ПДн субъекта от неправомерного их использования или утраты обеспечивается Банком за счет его средств в порядке, установленном комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» СТО БР ИББС и требованиями нормативных документов РФ.

13 ОБЯЗАННОСТИ, ПРАВА И ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ БАНКА ПРИ ОБРАБОТКЕ ПДН

Общее руководство и контроль над выполнением требований данного Положения возложены на ответственного за организацию обработки персональных данных в Банке и осуществление контроля за соблюдением требований Закона 152-ФЗ «О персональных данных».

Общая организация процессов обработки ПДн работников, членов семьи работников и кандидатов на вакантные должности в соответствии с установленными требованиями и непосредственное руководство указанными процессами в Банке.

Общая организация прочих процессов обработки ПДн (клиентов, представителей клиентов, контрагентов, контрагентов клиентов, выгодоприобретателей, посетителей) в соответствии с установленными требованиями и непосредственное руководство указанными процессами в Банке.

13.1. РУКОВОДИТЕЛИ ПОДРАЗДЕЛЕНИЙ БАНКА

13.1.1. Обязанности

В рамках процессов обработки ПДн руководители подразделений обязаны:

- обеспечивать выполнение требований по обработке и защите ПДн в соответствии с настоящим Положением и иными руководящими нормативными правовыми актами по защите ПДн;
- осуществлять постоянный контроль над подчиненными, разъяснять и требовать от подчиненных выполнения требований нормативных правовых актов по вопросам обработки и защиты ПДн;
- участвовать в процессе разработки и согласования организационно-распорядительных документов СЗПДн Банка;
- предоставлять необходимую информацию Начальнику отдела Информационной безопасности при проведении проверок регулирующими органами по вопросам обработки и обеспечения безопасности ПДн;
- определять необходимость и направлять на обучение Пользователей ПДн;
- предоставлять консультации Пользователям ПДн по вопросам автоматизированной и неавтоматизированной обработки ПДн в рамках своих компетенций;
- организовывать и контролировать своевременное предоставление работникам доступа к ПДн и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;
- определять права доступа к ПДн и автоматизированным средствам обработки ПДн в рамках своих компетенций;
- предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности ПДн;
- сообщать о выявленных нарушениях требований настоящего Положения Менеджеру по информационной безопасности ПДн и Администратору информационной безопасности ПДн.

13.1.2. Права

Руководители подразделений, участвующих в процессах обработки ПДн, имеют право:

- формировать предложения по совершенствованию СЗПДн Банка;
- формировать предложения о необходимости проведения контрольных мероприятий по защите ПДн для Менеджера по информационной безопасности ПДн;

- формировать предложения по внесению изменений в организационно-распорядительные документы СЗПДн Банка;
- запрашивать у работников, участвующих в обработке и обеспечении безопасности ПДн, информацию и документы, необходимые Руководителю в рамках обязанностей, указанных в п. 13.2.1.

13.2. РАБОТНИКИ БАНКА

13.2.1. Обязанности

Работники Банка, участвующие в процессах обработки ПДн, обязаны:

- соблюдать требования организационно-распорядительных документов СЗПДн Банка по обработке и обеспечению безопасности ПДн;
- проходить обучение и инструктаж по вопросам обработки и обеспечения безопасности ПДн;
- предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении внутренних контрольных мероприятий по защите ПДн;
- сообщать о выявленных нарушениях требований настоящего Положения своему непосредственному руководителю.

13.2.2. Права

Работники Банка, участвующие в процессах обработки ПДн, имеют право:

- получать доступ к ПДн в рамках выполнения своих трудовых обязанностей;
- получать консультации и рекомендации по вопросам обработки и обеспечения безопасности ПДн от должностных лиц, ответственных за обеспечение безопасности ПДн в Банке.