

Политика по обеспечению безопасности персональных данных в АО «ВУЗ - банк»

«Политика по обеспечению безопасности персональных данных АО «ВУЗ - банк» регулирует основные отношения, связанные с защитой персональных данных при их обработке, осуществляемой Банком.

Политика предъявляет требования к обеспечению безопасности персональных данных в информационных системах, устанавливает порядок реагирования на запросы от субъектов персональных данных и Уполномоченных органов по защите прав субъекта персональных данных, определяет ответственность за организацию, исполнение и контроль исполнения требований по защите персональных данных.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

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, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор – государственный либо муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие 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.

Обработка персональных данных

В Банке определен список подразделений, осуществляющих обработку персональных данных в информационных системах и имеющих доступ к персональным данным с целью исполнения своих должностных обязанностей.

Использование персональных данных Банком возможно только в соответствии с целями обработки персональных данных.

Обработка персональных данных в Банке производится как с применением средств автоматизации, так и без их применения.

Обработка персональных данных осуществляется Банком с согласия субъектов персональных данных за исключением следующего случая:

- Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия Банка.

Передача персональных данных Банком третьему лицу осуществляется с согласия субъекта персональных данных. В договоре о передаче персональных данных прописываются обязанности третьей стороны по обеспечению конфиденциальности персональных данных и безопасности персональных данных при их обработке.

При достижении целей обработки персональных данных Банк обязуется незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в сроки, установленные законодательством, если

иное не предусмотрено федеральными законами и отправить уведомление об уничтожении персональных данных.

Обработка запросов по персональным данным

Банк отвечает на запросы субъектов персональных данных (или их законных представителей) и Уполномоченных органов по защите прав субъекта персональных данных.

В банке существует единый, документально зафиксированный порядок обработки обращений субъектов персональных данных (или их законных представителей) по вопросам обработки их персональных данных и порядок обработки запросов по персональным данным Уполномоченного органа по защите прав субъекта персональных данных.

Защита персональных данных

Защита персональных данных — комплекс мер технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к субъекту персональных данных.

Защита персональных данных – прямая обязанность Банка как оператора персональных данных. Согласно действующему законодательству, Банк обязан обеспечить необходимый уровень защиты обрабатываемых им персональных данных:

- Банк при обработке персональных данных обязан принимать необходимые технические и организационные меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, изменения, уничтожения, копирования, блокирования, распространения персональных данных, а также от иных неправомерных действий.

Для построения целостной системы безопасности персональных данных в Банке определены основные цели и задачи защиты персональных данных. Главная цель защиты персональных данных - обеспечение конституционных прав граждан по сохранению личной тайны и конфиденциальности персональных данных, имеющих в информационных системах Банка. Задачами защиты персональных данных являются прогнозирование, своевременное выявление и устранение угроз носителям персональных данных.

Защита персональных данных в Банке осуществляется с соблюдением требований законодательства Российской Федерации в области персональных данных. Эти требования основаны на Конституции Российской Федерации и международных договорах Российской Федерации и состоят из Федерального закона №152 «О персональных данных» и других определяющих случаи и особенности обработки персональных данных федеральных законов, основным из которых является Федеральный закон «О банковской тайне».

Для обоснования, выбора и реализации мер по защите персональных данных в Банке определены и спрогнозированы возможные угрозы и оценены степени их опасности.

Требования к обеспечению безопасности персональных данных в информационных системах персональных данных

Комплекс мер по обеспечению безопасности персональных данных в информационных системах Банка предусматривает:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного уничтожения;
- доступ сотрудников Банка только к тем ресурсам информационных систем, которые необходимы для исполнения должностных обязанностей.
- контроль обработки персональных данных.
- работу в информационных системах только авторизованных пользователей;
- контроль, направленный на исключение возможности совершения злоумышленных действий;
- восстановление информации в случае ее умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники.

На всех сотрудников Банка, в том числе и сотрудников, осуществляющих обработку персональных данных, наложено обязательство соблюдения политик Банка по информационной безопасности.

В информационной системе Банка применяются сертифицированные средства антивирусной защиты.

Передача персональных данных по телекоммуникационным каналам и линиям связи между подразделениями организации, с одной стороны, и внешними организациями, с другой стороны, осуществляется с использованием сертифицированных СКЗИ или иных

защитных механизмов, применение которых определяется лицом, ответственным за обеспечение безопасности персональных данных в Банке.

Передача персональных данных между подразделениями Банка по телекоммуникационным каналам и линиям связи осуществляется только при обеспечении защиты персональных данных с помощью организации виртуальных частных сетей (VPN) или иных защитных мер, механизмов и средств, применение которых определяется лицом, ответственным за обеспечение безопасности персональных данных.

В Банке определена система контроля доступа, позволяющая осуществлять контроль доступа к коммуникационным портам, устройствам ввода вывода информации, съемным машинным носителям и внешним накопителям информации.

Администрирование систем защиты информации, применяемых в информационных системах, осуществляется квалифицированными специалистами, прошедшими обучение и имеющими опыт работы с ними.

Сотрудники Банка, допущенные к персональным данным, в обязательном порядке проходят соответствующее обучение аспектам обеспечения безопасности персональных данных и информационной безопасности.