Приложение № 7
к Положению об обработке персональных данных
в ООО КБ «Столичный Кредит»

ТРЕБОВАНИЯ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕАЛИЗУЕМЫЕ ООО КБ «СТОЛИЧНЫЙ КРЕДИТ»

1. Общество с ограниченной ответственностью Коммерческий Банк «Столичный Кредит» (далее - Банк) обеспечивает защиту обрабатываемых персональных данных от несанкционированного доступа и разглашения, неправомерного использования или утраты в соответствии с требованиями Федерального закона Российской Федерации № 152-ФЗ от 27.07.2006 г. «О персональных данных» со всеми изменениями и дополнениями, Постановления Правительства Российской Федерации № 687 от 15.09.2008 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановления Правительства Российской Федерации № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации № 512 от 06.07.2008 г. «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» со всеми изменениями и дополнениями, комплекса документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», а также рекомендаций Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации и Федеральной службы по техническому и экспортному контролю по вопросам соблюдения законодательных требований при обработке персональных данных.

2. При обработке персональных данных Банк принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3. Обеспечение безопасности персональных данных достигается, в частности, посредством:

- определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработки моделей угроз;
- применения 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;
- применения прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- проведения оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- организации учета машинных носителей персональных данных;

- обнаружения фактов несанкционированного доступа к персональным данным и принятия мер;
- восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установления правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечения регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

4. В целях обеспечения безопасности персональных данных, обрабатываемых без использования средств автоматизации, в отношении каждой категории персональных данных Банком определяются места хранения персональных данных (материальных носителей) и устанавливается перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. Банком обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Банком.

5. Использование и хранение биометрических персональных данных вне информационных систем персональных данных осуществляются Банком только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

6. Банком соблюдаются требования к технологиям хранения биометрических персональных данных вне информационных систем персональных данных и материальным носителям биометрических персональных данных, установленные Правительством Российской Федерации.

7. В целях исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при обработке персональных данных в информационных системах, Банк использует средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

8. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия. Классификация информационных систем персональных данных осуществляется Банком в порядке, установленном законодательством Российской Федерации.

9. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

10. Обрабатываемые в информационных системах персональные данные могут быть представлены для ознакомления:

- работникам Банка, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;
- уполномоченным лицам, осуществляющим обработку персональных данных по поручению Банка на основании заключенного с ним договора;
- уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

Работники, доступ которым к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании утвержденного Банком списка.

11. Запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется Начальником Отдела информационной безопасности. При обнаружении нарушений порядка предоставления персональных данных Банк незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

12. В целях реализации, эксплуатации, контроля и поддержания на должном уровне системы обеспечения информационной безопасности (СОИБ) Банка, снижения рисков нарушения информационной безопасности и управления ими в Банке создано Управление по информационной безопасности, подчиняющийся непосредственно исполнительному органу Банка. Начальник Управления информационной безопасности является должностным лицом, ответственным за организацию обработки Банком персональных данных и за выполнение законодательных требований при их обработке, а также за обеспечение информационной безопасности Банка.