CREDITEXPRESS

Утверждена Приказом
Генерального директора
Общества с ограниченной
ответственностью

«Кредитэкспресс Финанс»
№ 01-05ПД от 17.05.2018 г

ПОЛИТИКА ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

«КРЕДИТЭКСПРЕСС ФИНАНС» В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

(новая редакция)

Настоящий документ определяет политику Общества с ограниченной ответственностью «Кредитэкспресс Финанс» (далее – Общество) как оператора персональных данных, зарегистрированного 17.12.2012 г. за номером 77-12-000622 в Реестре операторов персональных данных Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в отношении обработки персональных данных.

Общество при обработке персональных данных руководствуется следующими основными правилами, определяющими его политику в отношении обработки персональных данных:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.

2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, 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 законодательством Российской Федерации.

8. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных ФЗ «О персональных данных». Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

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

3) обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;

4) обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее – исполнение судебного акта);

5) обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

6) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

7) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

8) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

9) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;

10) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке, а также в целях политической агитации, при условии обязательного обезличивания персональных данных;

11) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

12) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

9. Общество в своей деятельности осуществляет обработку персональных данных субъектов персональных данных из числа лиц, имеющих неисполненные обязательства перед контрагентами Общества или самим Обществом, исключительно в целях исполнения ими договоров, одной из сторон которых они являются, а также осуществления прав и законных интересов оператора или третьих лиц, в том числе в случаях, предусмотренных Федеральным законом «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях», обеспечивая конфиденциальность и безопасность таких данных. Обработка персональных данных иных лиц осуществляется в целях, указанных в согласии на обработку персональных данных таких лиц.

10. Общество обязано не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено ФЗ «О персональных данных».

11. Срок обработки персональных данных, в том числе срок их хранения определяется в согласии указанных лиц в случаях, когда такое согласие в соответствии с законодательством Российской Федерации необходимо для обработки персональных данных таких лиц.

12. В целях реализации политики Общества в отношении обработки персональных данных Общество реализует, в частности, следующие требования к защите персональных данных, в том числе из числа правовых, организационных и технических мер по обеспечению безопасности персональных данных, путем:

- назначения ответственного за организацию обработки персональных данных;

- издания документов, определяющих политику Общества в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Общества в отношении обработки персональных данных, локальным актам Общества;

- оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения ФЗ «О персональных данных», соотношение указанного вреда и принимаемых Обществом мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных»;

- ознакомления работников Общества, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Общества в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

- определения угроз безопасности персональных данных при их обработке в информационных системах персональных данных, формирование на их основе модели 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;

- оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учета машинных носителей персональных данных;

- обнаружения фактов несанкционированного доступа к персональным данным и принятием 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 обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных;

- организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечения сохранности носителей персональных данных;

- утверждения документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использования средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- назначения должностного лица (работник), ответственного за обеспечение безопасности персональных данных в информационной системе.

- предоставления доступа к содержанию электронного журнала сообщений исключительно для сотрудников Общества или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей;

- идентификации и аутентификации пользователей, являющихся сотрудниками Общества;

- идентификации и аутентификации устройств, в том числе стационарных, мобильных и портативных;

- управления идентификаторами, в том числе создания, присвоения, уничтожения идентификаторов;

- управления средствами аутентификации, в том числе хранения, выдачи, инициализации, блокирования средств аутентификации и принятия мер в случае утраты и (или) компрометации средств аутентификации;

- защиты обратной связи при вводе аутентификационной информации;

- идентификации и аутентификации пользователей, не являющихся сотрудниками Общества (внешних пользователей);

- управления (заведения, активации, блокирования и уничтожения) учетными записями пользователей, в том числе внешних пользователей;

- реализации необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

- управления (фильтрации, маршрутизации, контроля соединений, однонаправленной передачи и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;- разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;

- назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;

- ограничения неуспешных попыток входа в информационную систему (доступа к информационной системе);

- блокирования сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

- разрешения (запрета) действий пользователей, разрешенных до идентификации и аутентификации;

- реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

- регламентации и контроля использования в информационной системе технологий беспроводного доступа;

- регламентации и контроля использования в информационной системе мобильных технических средств;

- управления взаимодействием с информационными системами сторонних организаций (внешние информационные системы);

- обеспечения доверенной загрузки средств вычислительной техники;

- управления установкой (инсталляцией) компонентов программного обеспечения, в том числе определением компонентов, подлежащих установке, настройки параметров установки компонентов, контроля за установкой компонентов программного обеспечения;

- управления доступом к машинным носителям персональных данных;

- уничтожения (стирания) или обезличивания персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроля уничтожения (стирания) или обезличивания;

- определения событий безопасности, подлежащих регистрации, и сроков их хранения;

- определения состава и содержания информации о событиях безопасности, подлежащих регистрации;

- сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения;

- мониторинга (просмотра, анализа) результатов регистрации событий безопасности и реагирования на них;

- защиты информации о событиях безопасности;

- реализации антивирусной защиты;

- обновления базы данных признаков вредоносных компьютерных программ (вирусов);

- обнаружения вторжений;

- обновления базы решающих правил;

- выявления, анализа уязвимостей информационной системы и оперативного устранения вновь выявленных уязвимостей;

- контроля установки обновлений программного обеспечения, включая обновления программного обеспечения средств защиты информации;

- контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

- контроля состава технических средств, программного обеспечения и средств защиты информации;

- контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе;

- контроля целостности программного обеспечения, включая программного обеспечения средств защиты информации;

- обнаружения и реагирования на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама);

- периодического резервного копирования персональных данных на резервные машинные носители персональных данных;

- обеспечения возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала;

- идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

- управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

- регистрации событий безопасности в виртуальной инфраструктуре;

- управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

- контроля целостности виртуальной инфраструктуры и ее конфигураций;

- резервного копирования данных, резервирования технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;

- реализации и управления антивирусной защитой в виртуальной инфраструктуре;

- разбиения виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей;

- контроля и управления физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;

- размещения устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;

- разделения в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы;

- обеспечения защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

- обеспечения подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов;

- защиты архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных;

- разбиения информационной системы на сегменты (сегментирование информационной системы) и обеспечения защиты периметров сегментов информационной системы;

- защиты беспроводных соединений, применяемых в информационной системе;

- определения лиц, ответственных за выявление инцидентов и реагирование на них;

- обнаружения, идентификации и регистрации инцидентов;

- своевременного информирования лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

- анализа инцидентов, в том числе определения источников и причин возникновения инцидентов, а также оценка их последствий;

- принятия мер по устранению последствий инцидентов;

- планирования и принятия мер по предотвращению повторного возникновения инцидентов;

- определения лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных;

- управления изменениями конфигурации информационной системы и системы защиты персональных данных;

- анализа потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных;

- документирования информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных;

- проверки системного и (или) прикладного программного обеспечения, включая программного кода, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

- тестирования информационной системы на проникновения;

- использования в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищенного программирования;

- применения средств вычислительной техники не ниже 5 класса;

- применения системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;

- применения межсетевых экранов не ниже 3 класса;

- применения средств защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.