Утверждено
Приказом от «04» декабря 2015 г.

Положение о персональных данных
В ООО «Займинвест»

Содержание.

1. Общие положения.

1.1. Правовое регулирование обработки, защиты и обеспечения безопасности персональных данных.

Настоящее положение о персональных данных принято в соответствии с Конституцией Российской Федерации, «Конвенцией о защите физических лиц при автоматизированной обработке персональных данных» (заключена в г. Страсбурге 28.01.1981, ратифицирована Федеральным законом от 19.12.2005 № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»), Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

Обработка персональных данных в соответствии с настоящим Положением также регулируется Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указом Президента РФ от 06.03.1997 № 18 «Об утверждении перечня сведений конфиденциального характера».

Указанные нормативные правовые акты применяются с учетом всех изменений и дополнений, как принятых на дату издания настоящего Положения о персональных данных, так и принятых после издания настоящего Положения о персональных данных. В случае лишения указанных выше нормативных правовых актов юридической силы и принятия новых нормативных правовых актов, регулирующих обработку и защиту персональных данных, применяются вновь изданные нормативные правовые акты.

1.2. Основные понятия и термины.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (**субъекту персональных данных**).

Субъект персональных данных – физическое лицо, персональные данные которого обрабатываются Оператором в соответствии с законом о персональных данных, законодательством о персональных данных и настоящим Положением о 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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Неавтоматизированная обработка персональных данных - обработка персональных без использования средств вычислительной техники.

Согласие на обработку персональных данных – надлежащим образом оформленный письменный документ, в котором выражено согласие субъекта персональных данных с указанием целей обработки персональных данных, перечня персональных данных, оператора персональных данных, согласие субъекта персональных данных руководствоваться настоящим Положением при обработке его персональных данных и реализации прав субъекта персональных данных, предоставленных законом о персональных данных, иными актами о персональных данный и настоящим Положением, и иных условий, на которых осуществляется обработка 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. В соответствии с настоящим Положением оператором является ООО «Займинвест».

Передача персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Меры защиты персональных данных – комплекс организационных, технических и иных мер, которые оператор сочтет необходимыми для защиты персональных данных и обеспечения их безопасности, отвечающих требованиям законодательства о персональных данный и достаточных для защиты и обеспечения безопасности персональных данных.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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.

Законодательство о персональных данных – Конституция Российской Федерации, федеральные законы, указы Президента, постановления правительства, ведомственные акты и иные законы и подзаконные нормативные правовые акты, регулирующие порядок обработки и защиты персональных данных.

Закон о персональных данных - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

ФСТЭК - Федеральная служба по техническому и экспортному контролю Российской Федерации.

Роскомнадзор - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации.

Провайдер услуг по защите конфиденциальной информации – юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по защите конфиденциальной информации и имеющие соответствующие лицензии, которые оказали (оказывают) Оператору услуги по созданию комплекса программных и аппаратных средств, обеспечивающих сохранность и безопасность конфиденциальной информации в информационной системы, и поддержке указанного комплекса. Оператор может осуществлять указанные действия самостоятельно при наличии у него соответствующих лицензий.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Программное обеспечение - все или часть программ, процедур, правил и соответствующей документации системы обработки информации.

Системное программное обеспечение - комплекс программ, которые обеспечивают управление компонентами компьютерной системы, такими как процессор, оперативная память, устройства ввода-вывода, сетевое оборудование, выступая как «межслойный интерфейс», с одной стороны которого аппаратура, а с другой — приложения пользователя.

Прикладное программное обеспечение - программа, предназначенная для выполнения определённых задач и рассчитанная на непосредственное взаимодействие с пользователем.

1.3. Принципы обработки персональных данных.

При обработке персональных данных применяются следующие принципы:

1) Обработка персональных данных осуществляется на законной и справедливой основе.
2) Обработке подлежат только те персональные данные, и только в том объеме и в такие сроки, которые отвечают целям их обработки.
3) Персональные данные носят конфиденциальный характер и не подлежат разглашению третьим лицам.
4) При обработке персональных данных в одну информационную базу персональных данных могут быть систематизированы или консолидированы персональные данные, обработка которых осуществляется в одних и тех же или в смежных целях.
5) Обработка персональных данных не приведет к нарушению прав и законных интересов субъектов персональных данных, причинению вреда субъектам персональных данных.
6) Обработка персональных данных обеспечивает точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор принимает меры, необходимые для удаления или уточнения неполных или неточных данных.
7) 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.

1.4. Цели обработки персональных данных.

Обработка персональных данных осуществляется в связи с приобретением оператором прав требований к субъектам персональных данных по договорам займа, заключенным между ООО «Платиза.ру» - займодавцем - и субъектами персональных данных – заемщиками. Цели обработки персональных данных сводятся к исполнению договоров займа и реализации прав по договорам займа, в том числе реализации прав оператора на получение денежных потоков по договорам.

Для исполнения договоров займа и реализации прав по ним оператору необходимы персональные данные заемщиков, обеспечивающие коммуникации и взаимодействие с заемщиками, оценку платежеспособности заемщиков, информацию, необходимую для взыскания задолженности с заемщиков, в том числе в судебном порядке. Для реализации целей обработки персональных данных в соответствии с настоящим Положением о персональных данных требуются персональные данные, перечень которых указан в пункте 2.2. настоящего Положения.

2. Порядок обработки персональных данных.

2.1. Обработка персональных данных. Способы обработки персональных данных;

Обработка персональных данных состоит из следующих стадий:

1) Получение персональных данных оператором,
2) Обработка персональных данных,
3) Уничтожение или обезличивание персональных данных.

Получение персональных данных оператором. Оператор получает персональные данные субъектов персональных данных в связи с приобретением оператором прав требований к субъектам персональных данных по договорам займа у ООО «Платиза.ру» в соответствии с Договором уступки прав требования № 1 от 19.06.2015. Передача персональных данных осуществляется по защищенным телекоммуникационным каналам связи. Персональные данные передаются таким образом и с использованием таких механизмов и средств, которые обеспечивают защиту персональных данных от угроз безопасности персональных данных, приведенных в пункте 2.3. настоящего Положения о персональных данных.

Обработка персональных данных. Обработка персональных данных осуществляется комбинированным способом, в том числе с использованием технических средств и средств автоматизации.

Автоматизированная обработка персональных данных. По общему правилу, способ обработки персональных данных – автоматизированная обработка персональных данных. При обработке персональных данных в обычном режиме оператор осуществляет обработку персональных данных исключительно автоматизированным способом. Персональные данные хранятся на электронных носителях. Любая передача персональных данных (получение персональных данных, передача персональных данных между сотрудниками оператора, передача персональных данных третьим лицам) производится по электронным каналам связи. Оператор не переносит персональные данные на бумажные носители без необходимости. При автоматизированной обработке персональных данных оператор обеспечивает принятие всех необходимых организационных и технических мер защиты персональных данных.

Неавтоматизированная обработка персональных данных. Если для целей обработки персональных данных необходимо документировать персональные данные, включать персональные данные в какие-либо документы, оператор документирует персональные данные и (или) включает персональные данные в документы, в том числе в документы на бумажном носители. При неавтоматизированной обработке персональных данных оператор обеспечивает принятие всех необходимых мер защиты персональных данных.

Обработка персональных данных осуществляется путем сбора, хранения, накопления и систематизации персональных данных; систематизации персональных данных и включения их в базы данных аналогичных по составу и целям обработки персональных данных; анализа имеющихся персональных данных, поиска и подбора персональных данных и субъектов персональных данных по определенным признакам и (или) отвечающих определенным требованиям; изменения и обновления персональных данных; использования персональных данных при взаимодействии и коммуникации с заемщиками; обезличивания персональных данных; предоставления персональных данных субъектам персональных данных, к которым относятся такие данные, и совершения иных действий по запросам субъектов персональных данных в целях реализации прав субъектов персональных данных согласно законодательству о персональных данных; распространения и передачи персональных данных третьим лицам (при условии недопущения доступности персональных данных неопределенному кругу лиц и с учетом целей обработки персональных данных) в целях исполнения договоров займа; блокирования и уничтожения персональных данных.

Уничтожение или обезличивание персональных данных. Как только цели обработки персональных данных достигнуты, оператор обязуется уничтожить персональные данные. Если уничтожение персональных данных не возможно, оператор обязуется обезличить персональные данные.

Если оператору становится известно о недостоверности персональных данных, оператор обезличивает персональные данные, приостанавливает обработку персональных данных и предпринимает меры, необходимые для уточнения персональных данных. Обработка персональных данных не производится, и персональные данные хранятся в обезличенном виде до утонения и актуализации персональных данных.

Если в следствии уступки прав требования по договорам займа к субъектам персональных данных оператором на ООО «Платиза.ру» в соответствии с Договором уступки прав требования № 2 от 19.06.2015 или в силу иных обстоятельств отпадает необходимость обработки персональных данных отпадает, оператор обязуется уничтожить персональные данные. Если уничтожение персональных данных не возможно, оператор обязуется обезличить персональные данные.

Уничтожение и обезличивание персональных данных производится в соответствии с разделом 5 настоящего Положения о персональных данных.

2.2. Перечень персональных данных.

Оператор осуществляет обработку следующих персональных данных:

1) Фамилия, Имя, Отчество,
2) Сведения о дате и месте рождения,
3) Пол,

4) Сведения о месте жительства (проживания, пребывания),
5) Почтовый адрес,
6) Реквизиты основного документа, удостоверяющего личность,
7) Семейное положение,
8) Сведения об образовании,
9) Сведения о месте работы,
10) Сведения о профессии и должности,
11) Номера личного (мобильного), домашнего и рабочего телефонов,
12) Адрес электронной почты,
13) Сведения о заработной плате и ином доходе,
14) Сведения о непогашенных кредитах,
15) Сумма расходов по кредиту и сведения об иных расходах
16) Данные кредитной истории
17) ИНН,
18) Реквизиты СНИЛС,
19) Платежные реквизиты субъекта персональных данных.

2.3. Модель угроз безопасности персональных данных.

В целях формирования систематизированного перечня угроз безопасности персональных данных при их обработке в информационной системе персональных данных, угрозы безопасности персональным данным в информационной системе можно классифицировать в соответствии со следующими признаками:

1) по видам возможных источников угроз;
2) по типу информационной системы персональных данных, на которые направлена реализация угроз;
3) по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с персональными данными);
4) по способам реализации угроз;
5) по используемой уязвимости;
6) по объекту воздействия.

По видам возможных источников угроз безопасности персональных данных выделяют:
– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющими доступ к информационным ресурсам информационной системы персональных данных, включая пользователей;
– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к информационной системы персональных данных, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;
– угрозы, возникновение которых напрямую зависит от свойств техники, используемой в информационной системе персональных данных;
– угрозы, связанные с природными явлениями;
- угрозы, которые могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу информационной системы персональных данных, на которые направлена угроза, необходимо рассматривать следующие классы угроз:
– угрозы безопасности данных, обрабатываемых в информационной системе персональных данных на базе автоматизированных рабочих мест;
– угрозы безопасности данных, обрабатываемых в информационной системе персональных данных на базе локальных информационных систем;
– угрозы безопасности данных, обрабатываемых в информационной системе персональных данных на базе распределенных систем.

По способам реализации угроз выделяют следующие классы угроз:
– угрозы, связанные с несанкционированным доступом к персональным данным (в том числе угрозы внедрения вредоносных программ);
– угрозы утечки персональных данных по техническим каналам утечки информации;
– угрозы специальных воздействий на информационную систему персональных данных.

По виду нарушаемого свойства информации (несанкционированных действий, осуществляемых с персональными данными), можно выделить следующий класс угроз:
– угрозы, приводящие к нарушению конфиденциальности персональных данных (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации.

По используемой уязвимости выделяются следующие классы угроз:
– угрозы, реализуемые с использованием уязвимости системного программного обеспечения;
– угрозы, реализуемые с использованием уязвимости прикладного программного обеспечения;
– угрозы, возникающие в результате использования уязвимости, вызванной наличием в информационной системе персональных данных аппаратной закладки;
– угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
– угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации технической защиты информации от несанкционированного доступа;
– угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;
– угрозы, реализуемые с использованием уязвимостей средств защиты информации.

По объекту воздействия выделяются следующие классы угроз:
– угрозы безопасности персональных данных, обрабатываемых на автоматизированном рабочем месте;
– угрозы безопасности персональных данных, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т.п.);
– угрозы безопасности персональных данных, передаваемых по сетям связи;
– угрозы прикладным программам, с помощью которых обрабатываются персональных данных;
– угрозы системному программного обеспечения, обеспечивающему функционирование информационной системы персональных данных.

Также в целях применения законодательства о персональных данных и определения необходимого уровня защиты персональных данных, который устанавливается в отношении определенной информационной системы персональных данных, выделяют три типа угроз.

Угрозы первого типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы второго типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы третьего типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Для информационной системы персональных данных актуальны угрозы третьего типа, и, следовательно, в информационной системе персональных данных устанавливается третий уровень защищенности персональных данных (третий уровень защищенности в соответствии с пунктом 11 Постановления Правительства РФ от 01.11.2012 N 1119 «об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»).

2.4. Меры защиты и обеспечения безопасности персональных данных.

В соответствии с законом о персональных данных оператор определяет перечень мер защиты и обеспечения безопасности персональных данных. При определении перечня мер защиты и обеспечения безопасности персональных данных оператор исходит из состава актуальных угроз безопасности персональных данных.

Оператор обеспечивает соответствие мер защиты персональных данных объему персональных данных, целям обработки персональных данных, способам передачи персональных данных, угрозам безопасности персональных данных.

Оператор обеспечивает автоматизированную обработку персональных с использованием защищенных информационных систем, обеспечивающих защиту и безопасность персональных данных. В информационной системе персональных данных используются средства вычислительной техники не ниже 5 класса, системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса защиты, межсетевые экраны не ниже 3 класса в случае актуальности угроз 2-го типа.

Информационная система персональных данных, аппаратные и программные средства оператора в соответствии с разделом 4 настоящего Положения о персональных данных обеспечивают:

1) идентификацию и аутентификацию субъектов доступа и объектов доступа;
2) управление доступом субъектов доступа к объектам доступа исключительно ответственными уполномоченными лицами;
3) соответствующие ограничения программной среды;
4) защиту машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;
5) регистрацию сбоев и событий безопасности;
6) антивирусную защиту;
7) надлежащую работу системы обнаружения и предотвращения вторжений;
8) контроль (анализ) защищенности персональных данных;
9) целостность информационной системы и персональных данных;
10) доступность персональных данных уполномоченным лицам и субъектам персональных данных в пределах и в соответствии с регламентами и правилами, установленными законом о персональных данных и настоящим Положением о персональных данных;
11) защиту среды виртуализации;
12) защиту технических средств;
13) защиту информационной системы, ее средств, систем связи и передачи данных;
14) выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных и реагирование на них;
15) управление конфигурацией информационной системы и системы защиты персональных данных.

Для обработки и хранения персональных данных оператор создает в рамках информационной системы подсистемы и комплекс аппаратно-программных средств. Подсистемы обработки и хранения персональных данных функционируют в целях обработки, хранения и защиты персональных данных, однако отдельные компоненты и модули таких подсистем могут быть использованы в целях защиты иной информации в информационной системе. Выделяются подсистемы хранения персональных данных, анализа персональных данных, доступа сотрудников оператора к персональным данным в целях обработки, передачи персональных данных по внутренним каналам связи, передачи персональных данных внешним пользователям. Функционирование всех подсистем обеспечивает безопасность и защиту персональных данных в соответствии с законом о персональных данных, законодательством о персональных данных и настоящим Положением.

Различные подсистемы информационной системы персональных данных могут взаимодействовать, если это необходимо для защиты персональных данных, а также если взаимодействие подсистем не препятствует и не снижает уровень защиты персональных данных. Различные подсистемы информационной системы персональных данных взаимодействуют при реализации организационных мер защиты персональных данных. Также возможно взаимодействие различных подсистем информационной системы персональных данных путем использования смежных и сходных технологий, программных и аппаратных средств для обеспечения функционирования различных подсистем.

Оператор назначает лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных (см. Раздел 3.2. настоящего Положения о персональных данных). Оператор обеспечивает ознакомление сотрудников, осуществляющих обработку персональных данных и имеющих доступ к ним, с положениями закона о персональных данных, законодательства о персональных данных, настоящим Положением о персональных данных, а также нормами и стандартами информационной безопасности, нормами и стандартами защиты конфиденциальной информации и персональных данных.

Перечень персональных данных, подлежащий обработке, приведен в пункте 2.2. настоящего Положения о персональных данных. Перечень является исчерпывающим, и никакие иные персональные данные не подлежат обработке и хранению в информационной системе оператора.

Оператор обеспечивает конфиденциальность персональных данных. Конфиденциальность персональных данных обеспечивается путем установления и соблюдения режима конфиденциальности персональных данных, применения надлежащих технических мер защиты информации, в том числе защиты персональных данных от актуальных угроз безопасности персональных данных, ограничения доступа к персональным данным.

Оператор обеспечивает целостность информационной системы персональных данных, беспрерывность функционирования ее функционирования. Информационная система обеспечивает доступность персональных данных, неизменность и подлинность их содержания. Обработка персональных данных осуществляется в информационной системе оператора.

Информационная система персональных данных размещается на защищенных серверах на территории Российской Федерации. Работа с информационной системой персональных данных осуществляется с использованием защищенных каналов связи. Оператор обеспечивает защиту объектов информационной системы персональных данных от внешних угроз и физического воздействия.

Оператор организует и обеспечивает безопасность и защищенность носителей информации в информационных системах. Оператор предпринимает меры защиты носителей информации от угроз физического воздействия, несанкционированного доступа, проникновения, использования, порчи и повреждения. Оператор обеспечивает безопасность каналов, линий и средств связи и передачи данных.

При неавтоматизированной обработке персональных данных оператор обеспечивает документирование и обработку персональных данных уполномоченным лицом и полное соблюдение принципов конфиденциальности персональных данных, безопасное хранение персональных данных и документов, содержащих персональные данные, своевременное уничтожение документов, содержащих персональные данные.

2.5. Обеспечение прав субъектов персональных данных.

Субъект персональных данных имеет право на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных субъекта персональных данных, а также на ознакомление с такими персональными данными.

Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе:

1) подтверждение факта обработки персональных данных оператором;
2) правовые основания и цели обработки персональных данных;
3) цели и применяемые оператором способы обработки персональных данных;
4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;
5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения;
6) сроки обработки персональных данных, в том числе сроки их хранения;
7) порядок осуществления субъектом персональных данных прав, предоставленных законом о персональных данных;
8) информацию об осуществленной или о предполагаемой передаче персональных данных;
9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством о персональных данных меры по защите своих прав.

Сведения, которые должны быть предоставлены субъекту персональных данных в соответствии с настоящим разделом Положения о персональных данных, предоставляются

субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

По письменному запросу субъекту персональных данных или его законному представителю предоставляется доступ к персональным данным такого субъекта в течение 30 дней с момента получения запроса оператором. Доступ к персональным данным предоставляется при наличии технической возможности обеспечить безопасный доступ к персональным данным. Оператор в праве отказать субъекту персональных данных в предоставлении доступа к персональным данным, если невозможно обеспечить безопасное предоставление доступа к персональным данным. В таком случае, оператор предоставляет субъекту персональных данных информацию о составе персональных данных и порядке их обработке. Оператор также в праве отказать субъекту персональных данных в предоставлении доступа к персональным данным, если запрос на предоставление доступа к персональным данным не позволяет однозначно идентифицировать субъекта персональных данных, либо не подписан субъектом персональных данных.

Субъект персональных данных вправе ознакомиться с настоящим Положением о персональных данных. Если в документе, которым субъект персональных данных выражает свое согласие на обработку персональных данных, не указано иное, решения, порождающие юридически значимые последствия для субъекта персональных данных, могут приниматься в том числе на основании исключительно автоматизированной обработки персональных данных.

3. Организационные меры защиты и обеспечения безопасности персональных данных. Лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных.

Оператор обеспечивает и реализует ряд организационных мер защиты персональных данных, в частности, регламентирует порядок доступа к персональным данным и порядок их обработки назначает лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных и другие меры.

3.1. Организационные меры защиты персональных данных.

Оператор регламентирует порядок доступа и обработки персональных данных посредством принятия настоящего Положения о персональных данных, уведомления ответственных лиц, издание приказов и иных локальных нормативный актов и, при необходимости, подписания документов и получения письменных обязательств от своих сотрудников.

Оператор предоставляет доступ к персональным данным только если это необходимо для выполнения обязательств оператора и реализации прав оператора по договорам, стороной которых он является, и только тем лицам, которым доступ к персональным данным необходим для выполнения трудовых обязанностей. Оператор предоставляет доступ к персональным данным на условиях полной конфиденциальности персональных данных, о чем подписывается соответствующее соглашение. Такое соглашение может быть подписано в любой форме, в том числе посредством включения положений о конфиденциальности персональных данных в любые локальные акты и соглашения с сотрудниками.

Обработка персональных данных осуществляется в соответствии с пунктом 2.1. настоящего Положения о персональных данных при условии соблюдения всех мер защиты персональных данных, предусмотренных настоящим разделом. Обработка персональных данных осуществляется только уполномоченными лицами.

Оператор доводит до сведения сотрудников, непосредственно осуществляющих обработку персональных данных, положения законодательства о персональных данных, норм и стандартов обработки персональных данных. Оператор может устанавливать различные процедуры обработки персональных данных в рамках и во исполнении настоящего Положения о персональных данных, в том числе посредством оформления локального нормативного акта или устного разъяснения порядка обработки персональных данных.

Оператор организует ведение журналов и иных учетных документов, необходимый в связи с обработкой персональных данных в соответствии с применимым законодательством Российской Федерации. В частности оператор ведет учет материальных носителей персональных данных и их передачи сотрудникам оператора и третьим лицам.

Оператор уведомляет Роскомнадзор или иной уполномоченный государственный орган об обработке оператором персональных данных. Оператор организует хранение и соответствие всех документов, регламентирующих обработку персональных данных, действующему законодательству Российской Федерации. Оператор обеспечивает предоставление необходимых документов и материалов уполномоченным государственным органам при осуществлении ими контроля за реализацией мер защиты персональных данных и в иных случаях, предусмотренных законодательством Российской Федерации.

3.2. Лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных.

Оператор назначает лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных. Полномочия лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных, регламентируются настоящим пунктом Положения о персональных данных.

3.2.1. Порядок назначения лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных.

Лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных, назначается оператором посредством издания приказа о назначении лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных. Лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных, назначается на неопределенный срок. Полномочия лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных, прекращаются в случае прекращения трудовых отношений оператора с таким лицом, либо в случае назначения иного ответственного за организацию обработки, защиту и обеспечения безопасности безопасности персональных данных. Назначение другого ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных осуществляется посредством издания соответствующего приказа о прекращении полномочий ранее назначенного лица и назначении нового лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных.

3.2.2. Права и обязанности лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных.

Лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных обеспечивает:

1) Ознакомление сотрудников оператора с настоящим Положением о персональных данных;
2) Получение письменного обязательства о соблюдении конфиденциальности персональных данных и соблюдения правил их обработки от сотрудников оператора;
3) Публикацию настоящего Положения о персональных данных или доведение настоящего Положения о персональных данных до субъектов персональных данных иным образом;
4) Ведение учетных журналов и иных документов учета персональных данных;
5) Проведение контроля за соблюдением режима конфиденциальности персональных данных и реализации мер защиты персональных данных;
6) Реализацию мер защиты и обеспечения безопасности персональных данных.

4. Технические меры защиты персональных данных.

Технические меры защиты персональных данных представляют собой комплекс технических мер, позволяющих обеспечить защиту персональных данных в соответствии с пунктом 2.4. настоящего Положения о персональных данных. Технические меры защиты персональных данных реализуются посредством использования системы аппаратных и программных средств, обеспечивающих надлежащий уровень защиты персональных данных в соответствии с действующими стандартами и положениями законодательства Российской Федерации.

Меры идентификации и аутентификации. Меры по идентификации и аутентификации субъектов доступа и объектов доступа обеспечивают присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом. Меры по управлению доступом субъектов доступа к объектам доступа обеспечивают управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

Меры по ограничению программной среды. Меры по ограничению программной среды обеспечивают установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения и исключают возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

Меры по защите машинных носителей. Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) исключают возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

Меры по регистрации событий безопасности. Меры по регистрации событий безопасности обеспечивают сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите. Меры по антивирусной защите обеспечивают обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению и предотвращению вторжений. Меры по обнаружению (предотвращению) вторжений обеспечивают обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

Контрольные меры. Меры по контролю (анализу) защищенности персональных данных обеспечивают контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Меры по обеспечению целостности информационной системы. Меры по обеспечению целостности информационной системы и персональных данных обеспечивают обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

Меры по обеспечению доступности. Меры по обеспечению доступности персональных данных обеспечивают авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы, а также предоставление персональных данных и информации об обрабатываемых персональных данных субъектам персональных данных.

Меры по защите среды виртуализации. Меры по защите среды виртуализации исключают несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин, системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств. Меры по защите технических средств исключают несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы. Меры по защите информационной системы, в том числе средств, систем связи и передачи данных, обеспечивают защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

Меры реагирования. Меры по выявлению инцидентов и реагированию на них обеспечивают обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Меры по управлению конфигурацией. Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечивают управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Вышеуказанные меры реализуются посредством использования сертифицированного аппаратного и программного обеспечения, отвечающего требованиям применимого законодательства Российской Федерации и настоящего Положения о персональных данных. Оператор осуществляется обслуживание аппаратных и программных средств самостоятельно, либо привлекая сторонних провайдеров услуг, в том числе провайдеров услуг по защите конфиденциальной информации. В случае привлечения провайдеров услуг по защите конфиденциальной информации, оператор обеспечивает реализацию мер идентификации и аутентификации таких лиц, мер по управлению доступом в отношении таких лиц.

5. Порядок уничтожения и обезличивания персональных данных.

Персональные данные подлежат уничтожению в случае прекращения обработки персональных данных, по достижению целей обработки персональных данных или утрате актуальности целей обработки персональных данных. Уничтожение персональных данных является окончательным, и оператор не оставляет себе копий персональных данных.

Оператор осуществляет обработку персональных данных до истечение сроков исковой давности по договорам займа. Данный срок может быть продлен оператором, если законом установлена обязанность оператора персональных данных хранить персональные данные и (или) отдельные материалы и документы, содержащие персональные данные, в течение более длительного периода. Оператор также вправе продолжить хранить персональные данные, если имеются основания полагать, что обработка персональных данных будет возобновлена в ближайшее время, или появится необходимость хранить персональные данные в соответствии с законом.

Если цели обработки персональных данных достигнуты, сроки исковой давности по договорам займа истекли и основания для хранения персональных данных отсутствуют, оператор уничтожает персональные данные.

Уничтожение персональных данные, обработка которых осуществлялась автоматизированным способом, производится путем стирания (удаления) персональных данных с машинных, электронных и иных носителей информации способом, обеспечивающим невозможность восстановления персональных данных. Уничтожение персональных данных, обработка которых осуществлялась неавтоматизированным способом, осуществляется путем уничтожения документов и материалов, содержащих персональные данные способом, обеспечивающим невозможность прочтения таких документов и извлечения из них персональные данные.

Персональные данные подлежат обезличиванию, если необходимо уничтожить персональные данные, однако в силу объективных причин персональные данные невозможно

уничтожить, если персональные данные необходимо уничтожить, при этом сохранив документы и материалы, в которых содержатся персональные данные, а также если обработка персональных данных приостанавливается.

В результате обезличивания персональных данных невозможно определить принадлежность персональных данных конкретному субъекту персональных данных. Обезличивание персональных данных производится путем замены персональных данных идентификаторами. Оператор хранит словарь идентификаторов персональных данных в течение всего срока обезличивания персональных данных и до восстановления обработки персональных данных. Оператор обеспечивает сохранность словаря идентификаторов персональных данных и защиту их от несанкционированного доступа и использования.

6. Контроль за обработкой персональных данных, реализацией мер защиты и обеспечения безопасности персональных данных.

Контроль за реализацией мер защиты персональных данных осуществляется в регулярном режиме на постоянной основе. Оператор осуществляет внутренний контроль. Контроль за реализацией мер защиты персональных данных осуществляется в форме текущего контроля и регулярных внутренних проверок реализации мер защиты персональных данных.

Оператор в процессе своей деятельности осуществляет:

1) Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;

2) Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

3) Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;

4) Контроль состава технических средств, программного обеспечения и средств защиты информации;

5) Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе.

Оператор осуществляет контроль за реализацией мер защиты персональных данных самостоятельно, либо привлекает провайдеров услуг по защите конфиденциальной информации. Лицо, ответственное за организацию обработки, защиту и обеспечения безопасности персональных данных, осуществляет непосредственный контроль за реализацией мер защиты персональных данных и контролирует действия провайдеров услуг по защите конфиденциальной информации.

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе провайдеров услуг по защите конфиденциальной информации не реже одного раза в 3 года.

Также возможен внешний контроль за реализацией мер защиты персональных данных. Внешний контроль осуществляют уполномоченные государственные органы, и оператор гарантирует предоставление им всех документов и материалов, необходимых для осуществления контроля.

7. Заключительные положения.

Настоящее Положение о персональных данных вступает в силу с момента утверждения в день, указанный в соответствующем приказе.

Настоящее Положение о персональных данных принимается на неопределенный срок.

Настоящее Положение о персональных данных может быть опубликовано в сети Интернет на официальной Интернет - странице оператора, либо на иных Интернет – ресурсах.

Оператор вправе вносить изменения и дополнения в настоящее Положение о персональных данных в любой момент. В случае внесения изменений и (или) дополнений в настоящее Положение о персональных данных оператор уведомляет субъектов персональных данных об изменениях режима обработки персональных данных.

Оператор вправе отменить настоящее Положение о персональных данных и (или) заменить его другим Положением о персональных данных. В таком случае оператор уведомляет субъектов персональных данных об изменениях режима обработки персональных данных.

При изменении, дополнении или пересмотре настоящего Положения о персональных данных оператор обеспечивает включение в действующее Положение о персональных данных мер защиты персональных данных, обеспечивающих уровень защиты персональных данных не ниже предусмотренного настоящим Положением о персональных данных.

8. Приложения.

A. Форма согласия на обработку персональных данных;
B. Форма приказа о назначении лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных;
C. Инструкции лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных.

Приложение А.

Форма согласия на обработку персональных данных

1. Форма согласия на обработку персональных данных, выданного субъектом персональных данных лично.

В ООО «Займинвест»
ИНН 7727099210, ОГРН 1157746298423,
Адрес местонахождения: Россия, 115114, Москва, улица Летниковская, д. 10, стр. 4, комн. 50, 51 часть комн. 70

Согласие на обработку персональных данных

Я, *фамилия, имя, отчество*, проживающий по адресу: _____, *наименование и номер документа, удостоверяющего личность*, выдан _____ _____ г.,

Настоящим даю свое согласие на обработку моих персональных данных, перечень которых прилагается к настоящему согласию,

Обществу с ограниченно ответственностью «Займинвест», ИНН 7727099210, ОГРН 1157746298423, адрес местонахождения: Россия, 115114, Москва, улица Летниковская, д. 10, стр. 4, комн. 50, 51 часть комн. 70 (далее – «Оператор»)

в связи с приобретением Оператором прав требований ко мне по Договору займа № ____ от _____ (далее – «Договор») и в целях исполнения (реализации) прав Оператора по Договору («Цели обработки персональных данных»).

Под обработкой персональных данных понимается совершение любого из следующий действий или совокупности любых из таких действий в Целях обработки персональных данных, в том числе с использованием средств автоматизации, а именно: сбор, хранение, накопление и систематизация персональных данных; изменение и обновление персональных данных; систематизация моих персональных данных и включение их в базы данных персональных данных, обработка которых осуществляется в тех же или в аналогичных Целях; анализ имеющихся персональных данных, проверка персональных данных и меня, как субъекта персональных данных, по определенным признакам на предмет соответствия определенным требованиям; использование персональных данных для взаимодействия и коммуникации; обезличивание персональных данных; передача персональных данных третьим лицам в целях исполнения договоров между Оператором и третьими лицами; предоставление по моему запросу информации о составе и порядке обработке моих персональных данных и иные разумно необходимые действия с персональными данными в целях реализации прав субъекта персональных данных; блокирование и уничтожение персональных данных.

Настоящим я признаю, что мои персональные данные могут быть также использованы оператором в целях обеспечения моих прав в соответствии с Федеральным Законом «о персональных данных», и даю свое согласие на это.

Настоящим я подтверждаю, что:

А) мне знакомы нормы Федерального закона «о персональных данных» и иные положения законодательства Российской Федерации о защите персональных данных,

Б) насколько мне известно, Оператором принят документ, регламентирующий порядок обработки, защиты и обеспечения безопасности персональных данных с указанием мер мер защиты персональных данных (далее – «Положение о персональных данных»), и Оператор ознакомил меня с Положением о персональных данных и иными документами Оператора, регламентирующими защиту персональных данных,

В) положения Федерального закона «о персональных данных», иные положения законодательства Российской Федерации о защите персональных данных, Положение о персональных данных и иные документы Оператора, регламентирующие защиту персональных данных, мне известны и понятны,

Г) признаю, что Положение о персональных данных и иные документы Оператора, регламентирующие защиту персональных данных, регламентируют меры и процедуры, достаточные для защиты моих персональных данных и обеспечения их безопасности, а также полагаю, что процедуры реализации моих прав, возникающих в связи с обработкой персональных данных, установленные Положением о персональных данных и иными документами Оператора, регламентирующими защиту персональных данных, носят разумный характер, и буду следовать этим процедурам при реализации своих прав, возникающих в связи с обработкой персональных данных,

Д) Оператор вправе внести изменения и дополнения, а также пересмотреть Положение о персональных данных, и все изменения, дополнение и новые редакции Положения о персональных данных, если они не противоречат применимому законодательству, имеют силу и применяются к правоотношениям между мной и Оператором.

Настоящим даю свое согласие на обработку персональных данных до истечения срока исковой давности по Договору, либо реализации Целей обработки персональных данных (в зависимости от того, какое событие наступит позднее). Настоящее согласие может быть отозвано в порядке и сроки, предусмотренные законодательством Российской Федерации. Однако, я настоящим признаю, что Оператор вправе продолжить обработку моих персональных данных после отзыва настоящего согласия в соответствии с частью 2 статьи 9 и пунктом 7 части 1 статьи 6 Федерального закона «о персональных данных».

Дата:
Подпись:
Расшифровка:

Приложение
к согласию на обработку персональных данных

Перечень персональных данных, на обработку которых дается согласие:

1) Фамилия, Имя, Отчество,
2) Сведения о дате и месте рождения,
3) Пол,
4) Сведения о месте жительства (проживания, пребывания),
5) Почтовый адрес,
6) Реквизиты основного документа, удостоверяющего личность,
7) Семейное положение,
8) Сведения об образовании,
9) Сведения о месте работы,
10) Сведения о должности и профессии,
11) Номера личного (мобильного), домашнего и рабочего телефонов,
12) Адрес электронной почты,
13) Сведения о заработной плате и ином доходе,
14) Сведения о непогашенных кредитах,
15) Сумма расходов по кредиту и сведения об иных расходах,
16) Данные кредитной истории,
17) ИНН,
18) Реквизиты СНИЛС,
19) Платежные реквизиты субъекта персональных данных.

2. Форма согласия на обработку персональных данных, выданного представителем субъекта персональных данных.

В ООО «Займинвест»
ИНН 7727099210, ОГРН 1157746298423,
Адрес местонахождения: Россия, 115114, Москва, улица Летниковская, д. 10, стр. 4, комн. 50, 51 часть комн. 70

Согласие на обработку персональных данных

Я, *фамилия, имя, отчество*, проживающий по адресу: _____, *наименование и номер документа, удостоверяющего личность*, выдан _____ _____ г.,

Действующий на основании *доверенности* _____ в качестве представителя (далее – «Представитель») *фамилия, имя, отчество*, проживающего по адресу: _____, *наименование и номер документа, удостоверяющего личность*, выдан _____ _____ г. (далее «Субъект персональных данных)

Настоящим даю свое согласие на обработку персональных данных Субъекта персональных данных, перечень которых прилагается к настоящему согласию, а также на обработку моих персональных данных, указанных в настоящем согласии и приложении к нему,

Обществу с ограниченно ответственностью «Займинвест», ИНН 7727099210, ОГРН 1157746298423, адрес местонахождения: Россия, 115114, Москва, улица Летниковская, д. 10, стр. 4, комн. 50, 51 часть комн. 70 (далее – «Оператор»)

в связи с приобретением Оператором прав требований к Субъекту персональных данных по Договору займа № ____ от _____ (далее – «Договор») и в целях исполнения (реализации) прав оператора по Договору («Цели обработки персональных данных»).

Под обработкой персональных данных понимается совершение любого из следующий действий или совокупности любых из таких действий в Целях обработки персональных данных, в том числе с использованием средств автоматизации, а именно: сбор, хранение, накопление и систематизация персональных данных; изменение и обновление персональных данных; систематизация персональных данных и включение их в базы данных персональных данных, обработка которых осуществляется в тех же или в аналогичных Целях; анализ имеющихся персональных данных, поиск и подбор персональных данных и субъектов персональных данных по определенным признакам; использование персональных данных при взаимодействии и коммуникации с субъектом персональных данных; обезличивание персональных данных; передача персональных данных третьим лицам в целях исполнения договоров между Оператором и третьими лицами; предоставление субъекту персональных информации о составе и порядке обработке его персональных данных и иные разумно необходимые действия с персональными данными в целях реализации прав субъекта персональных данных; блокирование и уничтожение персональных данных.

Настоящим я признаю, что персональные данные могут быть также использованы оператором в целях обеспечения прав Субъекта персональных данных в соответствии с Федеральным Законом «о персональных данных», и даю свое согласие на это.

Настоящим я подтверждаю, что:

А) мне знакомы нормы Федерального закона «о персональных данных» и иные положения законодательства Российской Федерации о защите персональных данных,

Б) насколько мне известно, Оператором принят документ, регламентирующий порядок обработки, защиты и обеспечения безопасности персональных данных с указанием мер мер защиты персональных данных (далее – «Положение о персональных данных»), и Оператор ознакомил меня с Положением о персональных данных и иными документами Оператора, регламентирующими защиту персональных данных,

В) положения Федерального закона «о персональных данных», иные положения законодательства Российской Федерации о защите персональных данных, Положение о персональных данных и иные документы Оператора, регламентирующие защиту персональных данных, мне известны и понятны,

Г) признаю, что Положение о персональных данных и иные документы Оператора,

регламентирующие защиту персональных данных, регламентируют меры и процедуры, достаточные для защиты персональных данных и обеспечения их безопасности, а также полагаю, что процедуры реализации прав Субъекта персональных данных, возникающих в связи с обработкой персональных данных, установленные Положением о персональных данных и иными документами Оператора, регламентирующими защиту персональных данных, носят разумный характер, и буду следовать этим процедурам при реализации прав Субъекта персональных данных, возникающих в связи с обработкой персональных данных,

Д) Оператор вправе внести изменения и дополнения, а также пересмотреть Положение о персональных данных, и все изменения, дополнение и новые редакции Положения о персональных данных, если они не противоречат применимому законодательству, имеют силу и применяются к правоотношениям между Субъектом персональных данных и Оператором,

Е) я уполномочен(а) давать согласие на обработку персональных данных от имени Субъекта персональных данных, действовать от имени Субъекта персональных данных в целях защиты его персональных данный и соответствующих прав и законных интересов. Я уполномочен(а) делать заявления и давать подтверждения по указанным выше вопросам от имени Субъекта персональных данных и несу ответственность перед Субъектом персональных данных по всем вопросам, возникающим в связи с дачей настоящего согласия.

Настоящим даю согласие на обработку персональных данных Субъекта персональных данных до истечения срока исковой давности по Договору, либо реализации Целей обработки персональных данных. Настоящее согласие может быть отозвано в порядке и сроки, предусмотренные законодательством Российской Федерации. Однако, я настоящим признаю, что Оператор вправе продолжить обработку персональных данных Субъекта персональных данных после отзыва настоящего согласия в соответствии с частью 2 статьи 9 и пунктом 7 части 1 статьи 6 Федерального закона «о персональных данных».

Дата:
Подпись:
Расшифровка:

Приложение к согласию на обработку персональных данных

Перечень персональных данных, на обработку которых дается согласие:

Перечень персональных данных Субъекта персональных данных:

1) Фамилия, Имя, Отчество,
2) Сведения о дате и месте рождения,
3) Пол,
4) Сведения о месте жительства (проживания, пребывания),
5) Почтовый адрес,
6) Реквизиты основного документа, удостоверяющего личность,
7) Семейное положение,
8) Сведения об образовании,
9) Сведения о месте работы,
10) Сведения о должности и профессии,
11) Номера личного (мобильного), домашнего и рабочего телефонов,
12) Адрес электронной почты,
13) Сведения о заработной плате и ином доходе,
14) Сведения о непогашенных кредитах,
15) Сумма расходов по кредиту и сведения об иных расходах
16) Данные кредитной истории,
17) ИНН,
18) Реквизиты СНИЛС,
19) Платежные реквизиты субъекта персональных данных.

Перечень персональных данных Представителя:

1) Фамилия, Имя, Отчество,
2) Сведения о дате и месте рождения,
3) Пол,
4) Сведения о месте жительства (проживания, пребывания),
5) Почтовый адрес,
6) Реквизиты основного документа, удостоверяющего личность,
7) Номера личного (мобильного), домашнего и рабочего телефонов,
8) Адрес электронной почты.

Приложение В.

Форма приказа о назначении лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных

На бланке оператора

Приказ

Москва дата приказа

В соответствии с пунктом 1 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»и принятыми в соответствии с ним нормативными правовыми актами, приказываю:

1. Назначить _____ответственным за организацию обработки, защиты и обеспечение безопасности персональных данных в ООО «Займинвест»
2. Утвердить инструкции для лица, ответственного за организацию обработки, защиты и обеспечение безопасности персональных данных (Приложение 1).
3. Контроль за исполнением настоящего Приказа оставляю за собой.

Генеральный директора ООО «Займинвест»
Кузнец И.В.

С Приказом ознакомлен(а):

_____/ _____/
(подпись) (расшифровка подписи)

« » _____20_____г.

Приложение С.

Инструкции лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных.

На бланке оператора

Приложение № 1
К Приказу от _____

Инструкции лица, ответственного за организацию обработки, защиту и обеспечения безопасности персональных данных

1. Общие положения.

1.1. Инструкции лица, ответственного за организацию обработки, защиты и обеспечения безопасности персональных данных в ООО «Займинвест» (далее - Инструкция), разработана в соответствии с пунктом 1 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»и принятыми в соответствии с ним нормативными правовыми актами.
1.2. Настоящая Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки, защиты и обеспечения безопасности персональных данных в ходе исполнения и реализации ООО «Займинвест» прав на денежные потоки по договорам займа.
1.3. Лицо, ответственное за организацию обработки, защиты и обеспечения безопасности персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, Положением о персональных данных ООО «Займинвест» от _____ и настоящей Инструкцией.

2. Обязанности лица, ответственного за организацию обработки, защиты и обеспечения безопасности персональных данных.

Лицо, ответственное за организацию обработки, защиты и обеспечение безопасности персональных данных обязано:
2.1. Осуществлять внутренний контроль за соблюдением сотрудниками ООО «Займинвест» законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.
2.2. Доводить до сведения сотрудников ООО «Займинвест» положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.
2.3. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой указанных обращений и запросов.

3. Права лица, ответственного за организацию обработки персональных данных в организации.

Лицо, ответственное за организацию обработки персональных данных, имеет право:
3.1. Принимать решения в пределах своей компетенции.
3.2. Требовать от сотрудников ООО «Займинвест» соблюдения действующего законодательства, а также локальных нормативных актов ООО «Займинвест» о персональных данных.
3.3. Контролировать других ответственных лиц, осуществляющих обработку персональных данных.
3.4. Взаимодействовать с государственными органами, физическими и юридическими лицами по вопросам обработки персональных данных.

4. Ответственность лица, ответственного за организацию обработки персональных данных в организации.

4.1. За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства о персональных данных лицо, ответственное за организацию обработки персональных данных в организации, несет предусмотренную законодательством Российской Федерации ответственность.

Лист ознакомления.

С инструкцией ознакомлен(а):

_____/ _____/
(подпись) (расшифровка подписи)

« » _____20_____г.