

**СОГЛАШЕНИЕ ОБ ИСПОЛЬЗОВАНИИ
АНАЛОГА СОБСТВЕННОРУЧНОЙ ПОДПИСИ
ПРИ ДИСТАНЦИОННОМ ВЗАИМОДЕЙСТВИИ
ООО МКК «Гульден»**

ОГЛАВЛЕНИЕ

1. Общие положения.
2. Термины и определения.
3. Предмет соглашения.
4. Порядок использования АСП.
5. Правила проверки электронной подписи.
6. Конфиденциальность.
7. Ответственность сторон.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее соглашение (далее – Соглашение) устанавливает порядок дистанционного взаимодействия между сторонами, а также условия использования Клиентом аналога собственноручной подписи в ходе обмена электронными документами между сторонами, определяет возникающие в этой связи права, обязанности и ответственность сторон.

1.2 Соглашение является типовым формуляром (договором присоединения) ООО МКК «Гульден» (далее – Общество) и может быть принято Клиентом не иначе как путем присоединения к Соглашению в целом в порядке, установленном Соглашением.

1.3 Присоединение к Соглашению осуществляется Клиентом в соответствии со статьями 428 и 438 Гражданского кодекса Российской Федерации (далее – ГК РФ) путем выполнения конклюдентных действий. Для целей настоящего Соглашения к таким действиям относятся, в частности, проставление отметки (галочки) в соответствующем поле (чек-боксе), нажатие кнопок или иных элементов интерфейса с обозначением «Подписать», «Подтвердить», «Согласен», «Продолжить», «Отправить», «Подать заявку», «Получить», а также совершение иных действий в интерфейсе Сайта Общества или личного кабинета Сайта и/или мобильного приложения (если это технически предусмотрено), которые по своему смыслу однозначно подтверждают волеизъявление пользователя на подписание электронного документа, принятие условий документа либо совершение иного юридически значимого действия.

1.4 Совершение пользователем действий, указанных в пункте 1.3 настоящего Соглашения, означает полное и безоговорочное согласие пользователя с условиями настоящего Соглашения.

1.5 Общество вправе в одностороннем порядке изменять (дополнять) условия настоящего Соглашения. Новая редакция Соглашения доводится до сведения Клиентов посредством ее опубликования на Сайте Общества. Клиент признается принявшим условия Соглашения в новой редакции, если после их вступления в силу он приступает к оформлению заявления о предоставлении займа/заявления о пролонгации договора займа/использует ключ электронной подписи в порядке, предусмотренном Правилами предоставления займов Общества и настоящим Соглашением. Указанные действия рассматриваются Обществом в качестве конклюдентных действий, свидетельствующих о выражении Клиентом согласия на принятие новой редакции Соглашения.

1.6. Настоящее Соглашение подлежит применению ко всем электронным документам и юридически значимым действиям, совершаемым пользователем с использованием сайта Общества и (или) личного кабинета, если иной порядок прямо не установлен законом, отдельным соглашением сторон либо существом соответствующего правоотношения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1 Перечисленные в настоящем пункте и используемые в настоящем Соглашении термины и выражения имеют следующее значение:

АСП – аналог собственноручной подписи, в качестве которого рассматривается простая электронная подпись, формируемая в соответствии с требованиями Соглашения и законодательства Российской Федерации;

Договор займа – договор потребительского займа, заключенный Обществом и Клиентом в порядке, определенном Правилами предоставления займов Общества;

Закон об электронной подписи – Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» в действующей редакции;

Зарегистрированный номер – номер мобильного телефона Клиента, указанный и подтвержденный Клиентом в порядке, установленном Правилами предоставления займов общества;

Клиент – физическое лицо, желающее присоединиться и/или присоединившееся к условиям Соглашения;

Конклюдентные действия - действия пользователя, совершаемые им на Сайте, в личном кабинете или с использованием иных технических средств Общества, которые прямо предусмотрены интерфейсом Сайта, правилами использования соответствующего сервиса либо настоящим Соглашением и которые по своему содержанию однозначно выражают волю пользователя на присоединение к Соглашению, подписание электронного документа, подтверждение согласия, направление заявки, совершение платежа либо иное юридически значимое действие;

Личный кабинет – поддерживаемая Обществом информационная подсистема Сайта, представляющая собой личную страницу Клиента по адресу <https://mkkgulden.ru/> и/или мобильного приложения (если это технически предусмотрено), которая позволяет Клиенту и Обществу осуществлять дистанционное взаимодействие в электронной форме;

Логин – символьное обозначение, совпадающее с Зарегистрированным номером Клиента, используемое для аутентификации Клиента в целях предоставления ему доступа к Личному кабинету;

Общество – Общество с ограниченной ответственностью Микрокредитная компания «Гульден», ОГРН 1257700154887, регистрационный номер записи в государственном реестре микрофинансовых организаций 2503045010162, место нахождения: - 107150, Г.МОСКВА, ВН.ТЕР.Г. МУНИЦИПАЛЬНЫЙ ОКРУГ БОГОРОДСКОЕ, УЛ БОЙЦОВАЯ, Д. 17, К. 1, ПОМЕЩ. 4/1;

Пароль – конфиденциальное символьное обозначение, предоставленное Клиенту в процессе получения доступа к Личному кабинету или определенное им впоследствии, и используемое для аутентификации Клиента в целях предоставления ему доступа к Личному кабинету;

Правила - Правила предоставления займов Общества;

Сайт – сайт Общества в сети «Интернет», доступ к которому осуществляется по адресу <https://mkkgulden.ru/>;

СМС-код – предоставляемый Клиенту посредством СМС-сообщения уникальный конфиденциальный символьный код, который представляет собой ключ электронной подписи в значении, придаваемом данному термину п. 5 ст. 2 Закона об электронной подписи. СМС-код используется Клиентом для подписания электронных документов в ходе дистанционного взаимодействия с Обществом;

Система – совокупность программных средств, используемых Обществом в целях поддержания функционирования Личного кабинета, обеспечения информационного обмена между Клиентом и Обществом, а также автоматического протоколирования (логирования) действий, совершаемых Клиентами в Личном кабинете;

Аутентификация - установление принадлежности Клиента прав доступа к Системе в соответствии с предъявленным им средством аутентификации.

Средства аутентификации - логин, пароль, ПИН-код, СМС-код, Touch ID, Face ID и иные технические средства, используемые Обществом для подтверждения факта доступа пользователя к личному кабинету и совершения им действий на Сайте.

Face ID - это технология биометрической аутентификации для распознавания лица Клиента.

Touch ID - это технология биометрической аутентификации для распознавания отпечатка пальца Клиента.

ПИН-код - секретная числовая комбинация, устанавливаемая Клиентом самостоятельно и используемая для идентификации Клиента.

Сторона или Стороны – Клиент и Общество, упоминаемые по отдельности или вместе.

Иные термины и выражения, используемые в настоящем Соглашении, имеют значение, которое придается им в законах, иных нормативных актах Российской Федерации, а также в Правилах.

3. ПРЕДМЕТ СОГЛАШЕНИЯ

3.1 Настоящее Соглашение определяет порядок дистанционного взаимодействия между Сторонами, а также условия использования Клиентом АСП в ходе обмена электронными документами между Сторонами, а также для заключения, изменения и исполнения ими Договора займа, подписания электронных документов при взаимодействии Сторон. Кроме того, настоящее Соглашение определяет права и обязанности Сторон, возникающие в связи с формированием, отправкой и получением электронных документов с использованием Личного кабинета.

3.2 В целях обеспечения возможности электронного взаимодействия между Сторонами Общество предоставляет Клиенту ключи электронной подписи, ведет и обновляет реестр выданных ключей, поддерживает функционирование Системы, а также совершает иные действия, предусмотренные настоящим Соглашением.

4. ПОРЯДОК ИСПОЛЬЗОВАНИЯ АСП

4.1 В соответствии с частью 2 статьи 160 Гражданского кодекса Российской Федерации и частью 2 статьи 6 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» стороны признают, что электронные документы и юридически значимые действия, совершенные с соблюдением требований настоящего Соглашения, считаются подписанными АСП пользователя и влекут для сторон те же правовые последствия, что и документы на бумажном носителе, подписанные собственноручной подписью.

4.2. Электронный документ считается подписанным АСП пользователя, а пользователь – совершившим соответствующее юридически значимое действие, если соблюден один из следующих способов подтверждения волеизъявления пользователя:

4.2.1. в электронный документ либо в сведения Системы, относящиеся к соответствующему электронному документу, включен цифровой идентификатор, равнозначный СМС-коду, направленному пользователю на зарегистрированный номер и впоследствии введенному пользователем в специальное интерактивное поле на Сайте или в личном кабинете;

4.2.2. пользователь совершил конклюдентное действие, прямо предусмотренное интерфейсом Сайта или личного кабинета как действие, подтверждающее подписание электронного документа, принятие его условий, выражение согласия либо совершение иного юридически значимого действия, при условии фиксации такого действия Системой.

4.2.3. пользователь подтвердил волеизъявление путём прохождения процедуры аутентификации в интерфейсе Сайта или личного кабинета с использованием Face ID, Touch ID либо ПИН-кода, при условии, что такой способ аутентификации был предварительно согласован пользователем и зафиксирован Системой.

4.3. СМС-код направляется на зарегистрированный номер пользователя и считается предоставленным лично пользователю. Пользователь признает и соглашается, что получение СМС-кода на зарегистрированный номер подтверждает возможность использования указанного номера в качестве средства формирования АСП.

4.4. СМС-код может использоваться пользователем для подписания электронного документа и (или) комплекта электронных документов, а также для подтверждения совершения иных действий, доступных пользователю в интерфейсе Сайта или личного кабинета. СМС-код действителен для подписания электронных документов и (или) совершения соответствующего юридически значимого действия в течение 30 (Тридцати) календарных дней с момента его направления пользователю, если более короткий срок действия такого СМС-кода не установлен техническими настройками Системы, о чем пользователю сообщается в интерфейсе Сайта, личного кабинета либо в сообщении, содержащем СМС-код.

4.5. Неиспользование СМС-кода в течение срока его действия означает истечение срока действия соответствующего ключа простой электронной подписи. Для подписания электронного документа или совершения иного действия после истечения срока действия СМС-кода пользователь получает новый СМС-код в порядке, предусмотренном Системой.

4.6. До подписания электронного документа пользователю обеспечивается техническая возможность ознакомиться с его содержанием на Сайте, в личном кабинете либо иным способом, предусмотренным соответствующим интерфейсом электронного сервиса. Совершение пользователем действий по подписанию документа подтверждает, что пользователь с таким документом ознакомился в объеме, достаточном для понимания его содержания и правовых последствий его подписания.

4.7. Любое заявление, согласие, подтверждение, уведомление, заявка, информационное сообщение либо иной электронный документ, подписанный АСП пользователя в порядке, предусмотренном настоящим Соглашением, признается документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью пользователя.

4.8. Датой и временем подписания электронного документа и (или) совершения соответствующего юридически значимого действия признаются дата и время, зафиксированные Системой.

4.9. В рамках настоящего Соглашения использование ПИН-кода, Face ID, Touch ID признается применением АСП для целей подтверждения волеизъявления Клиента и придания электронным документам юридической силы. При этом математическая модель лица, отпечатков пальцев формируется и обрабатывается исключительно на устройстве Клиента в изолированной среде и не передаётся, не хранится и не обрабатывается на серверах или в инфраструктуре Сервиса.

4.10. Перед первым подключением Face ID, Touch ID и/или ПИН-кода Пользователь обязан явно выразить согласие на использование технологий Face ID, Touch ID, ПИН-код для аутентификации Общества (далее – Соглашение). Процедура получения согласия предусматривает:

4.10.1. отображение отдельного информационного блока с разъяснением цели, состава и правовых оснований Соглашения;

4.10.2. выбор действия «Согласен»/«Не согласен» в виде отдельной кнопки или чекбокса, не объединённого с иными согласиями и не являющегося частью общего согласия на обработку персональных данных;

4.10.3. прохождение дополнительного подтверждения волеизъявления путём ввода одноразового кода, направленного на номер телефона, указанный Пользователем при регистрации в Сервисе (СМС код). Ввод корректного СМС кода является обязательным условием признания согласия действительным;

4.10.4. фиксацию факта согласия в логах Сервиса с привязкой к учётной записи и сессии, включая: время и дату события, IP адрес, идентификатор устройства, тип канала получения СМС, факт ввода кода и его успешную валидацию.

4.11. Соглашение считается предоставленным только после совершения Пользователем совокупности активных действий, подтверждающих волеизъявление: нажатие кнопки/отметка чекбокса «Согласен» и последующий ввод корректного СМС кода. Простое продолжение использования Сервиса без явного акцепта и подтверждения СМС кодом не является Соглашением.

5. ПРАВИЛА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

5.1. Факт подписания электронного документа АСП пользователя устанавливается Обществом путем сопоставления сведений, содержащихся в Системе, в том числе с использованием электронных журналов, реестров, записей информационного обмена и иных технических данных.

5.2. При использовании СМС-кода факт подписания электронного документа или подтверждения совершения иного действия устанавливается путем сопоставления, в частности, следующих сведений:

5.2.1. СМС-кода (цифрового идентификатора), использованного при подписании электронного документа и (или) подтверждении действия;

5.2.2. сведений о направлении соответствующего СМС-кода на зарегистрированный номер пользователя;

5.2.3. информации о зарегистрированном номере, указанном за соответствующим пользователем в Системе;

5.2.4. технических данных об активности пользователя на Сайте и (или) в личном кабинете, автоматически зафиксированных в электронных журналах Системы, включая сведения о дате, времени, IP-адресе, параметрах сессии, браузере, устройстве и иных данных, доступных Обществу в рамках функционирования Системы;

5.2.5. иных сведений, позволяющих достоверно установить факт совершения пользователем соответствующего действия.

5.3. При использовании конклюдентных действий факт подписания электронного документа или подтверждения совершения иного действия устанавливается путем сопоставления, в частности, следующих сведений:

5.3.1. информации о совершении пользователем конкретного действия в интерфейсе Сайта или личного кабинета;

5.3.2. сведений о содержании интерфейсного элемента, посредством которого было совершено соответствующее действие;

5.3.3. сведений учетной записи пользователя и параметров сессии, в рамках которой было совершено действие;

5.3.4. технических данных, автоматически зафиксированных Системой, включая дату, время, IP-адрес, сведения об устройстве, браузере и иные релевантные технические параметры;

5.3.5. иных сведений, содержащихся в Системе и подтверждающих факт совершения пользователем соответствующего действия.

5.4. Общество осуществляет хранение электронных документов, созданных, направленных, подписанных, полученных или подтвержденных пользователем в процессе использования Сайта, личного кабинета и Системы, а также хранение сведений о юридически значимых действиях пользователя, включая логи и иные технические данные, необходимые для подтверждения факта подписания электронных документов и совершения соответствующих действий.

5.5. Сведения, содержащиеся в Системе, включая электронные журналы, логи, данные о выдаче и использовании СМС-кодов, сведения о действиях пользователя в интерфейсе Сайта и личного кабинета, признаются сторонами надлежащими и достаточными доказательствами факта формирования, направления, получения, подписания электронного документа и (или) совершения пользователем соответствующего юридически значимого действия.

5.6. Проверка электронной подписи, сформированной в Системе с применением ПИН кода, Face ID, Touch ID осуществляется в следующем порядке:

5.6.1. Проверка криптографической корректности электронной подписи и статуса сертификата. При проверке подписи осуществляется верификация математической целостности подписи в отношении содержимого документа (путём сопоставления криптографического хэша документа и результата проверки подписи с использованием открытого ключа). Одновременно проверяется действительность сертификата открытого ключа на момент формирования подписи: отсутствие истечения срока действия сертификата, отсутствие сведений об отзыве сертификата в списках отозванных сертификатов (CRL), соответствие сертификата установленным требованиям к сертификатам ключей проверки электронной подписи.

5.6.2. Проверка фактора аутентификации, использованного для подтверждения права на применение закрытого ключа. Система проверяет корректность подтверждения личности владельца ключа в соответствии с выбранным фактором:

при использовании ПИН-кода — соответствие введенного значения значению, зарегистрированному в профиле аутентификации, с учётом установленных ограничений на количество попыток ввода;

при использовании Face ID или Touch ID — наличие подтверждённого системой устройства результата успешной биометрической верификации (сигнала «аутентификация успешна»), сформированного в рамках защищённого контура устройства без передачи биометрических образцов за пределы устройства.

5.6.3. Проверка целостности и неизменности подписываемого документа в процессе подписания. Осуществляется контроль соответствия документа, фактически подписанного электронной подписью, документу, представленному пользователю для ознакомления и подтверждения на этапе инициации подписания. Проверяется отсутствие подмены содержимого документа на промежуточных этапах подписания, а также соответствие идентификаторов документа (включая хэш) в метаданных подписи и в исходных данных операции.

5.6.4. Фиксация результатов проверки. Система регистрирует результат (успех или причина отказа), использованный фактор аутентификации, временную метку операции, идентификатор сессии и другие релевантные данные. Эта информация подлежит обязательной записи в журнал аудита информационной системы для последующего анализа и расследования инцидентов.

5.7. Предусмотренный настоящим разделом порядок установления лица, создавшего и подписавшего электронный документ либо совершившего юридически значимое действие, признается сторонами достаточным для достоверной идентификации пользователя и подтверждения его волеизъявления.

6. КОНФИДЕНЦИАЛЬНОСТЬ

6.1 Клиент обязан:

– не разглашать любым третьим лицам информацию о закреплённом за ним Логине, Пароле и конфиденциальном СМС-коде, полученном Клиентом в целях формирования АСП, а также предпринимать все меры, необходимые для сохранения этих сведений в тайне;

– не передавать третьим лицам СИМ-карту, которая обеспечивает возможность использовать Зарегистрированный номер, а также предпринимать все меры, необходимые для того, чтобы третьи лица не получили возможность использования указанной СИМ-карты без осуществления контроля со стороны Клиента;

– незамедлительно сообщать Обществу о нарушении секретности сведений, указанных выше, а также о возникновении у Клиента подозрений в нарушении их секретности или об утрате Клиентом контроля над СИМ-картой.

6.2 Сообщение, указанное в п. 6.1, необходимо направить Обществу посредством отправки электронного сообщения на адрес info@mkkgulden.ru (сообщение должно содержать копию паспорта Клиента).

6.3 Клиент несет ответственность за сохранность средств аутентификации. Общество несет ответственность за

- Функционирование Системы;
- Корректную генерацию и доставку СМС-кодов;
- Защиту информации в рамках своей зоны контроля.

Риски распределяются между Сторонами с учетом фактических обстоятельств и доказанности вины.

6.4 Система обеспечивает конфиденциальность информации об СМС-коде (ключе электронной подписи) Клиента. Сведения о Логине, СМС-коде и Пароле, которые закреплены за Клиентом, доступны исключительно уполномоченным сотрудникам Общества.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1 Стороны несут ответственность за невыполнение или ненадлежащее выполнение своих обязательств по настоящему Соглашению в пределах суммы причиненного другой Стороне реального ущерба.

7.2 Стороны несут ответственность за неисполнение или надлежащее исполнение своих обязательств по настоящему Соглашению, если не будет доказано, что соответствующее нарушение допущено не по вине Стороны.

7.3 Стороны не несут ответственность за неисполнение либо ненадлежащее исполнение своих обязательств по настоящему Соглашению, если соответствующее нарушение обусловлено ненадлежащим исполнением своих обязательств другой Стороной или вызвано действием обстоятельств непреодолимой силы.