ЧАСТЬ А. РЕГЛАМЕНТ УЦ И ЭЛЕКТРОННОЙ ПОДПИСИ

К Пользовательскому соглашению (часть А — регламент сервиса) и Политике обработки персональных данных (часть В) · редакция от 30.09.2026

А1. Термины и определение Сервиса

1.1. **Сервис «Подпись»** — функциональный модуль Экосистемы, обеспечивающий выпуск ключей и сертификатов электронной подписи, формирование электронной подписи документов и сообщений, а также проверку подписи и статуса сертификатов.

1.2. **УЦ Gramaton** — удостоверяющий центр Оператора, обеспечивающий выпуск и сопровождение сертификатов электронной подписи в инфраструктуре Экосистемы. УЦ построен по иерархии «корневой сертификат → выпускающий сертификат → сертификаты участников».

1.3. **Электронная подпись (ЭП)** — информация в электронной форме, которая присоединена к другой информации в электронной форме и используется для определения лица, подписывающего информацию (ст. 2 Федерального закона от 06.04.2011 № 63-ФЗ, далее — «Закон № 63-ФЗ»).

1.4. **Виды подписи в Сервисе:**

1.4.1. **Простая электронная подпись (ПЭП)** — подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования подписи определённым лицом; используется для подтверждения действий Пользователя в интерфейсах Сервисов; 1.4.2. **Усиленная неквалифицированная электронная подпись (УНЭП)** — подпись, полученная в результате криптографического преобразования информации с использованием ключа, позволяющая определить подписавшее лицо и обнаружить изменения документа; формируется на ключе, выпущенном УЦ Gramaton (криптография стандарта организации); 1.4.3. **Усиленная квалифицированная электронная подпись (УКЭП)** — подпись, соответствующая требованиям Закона № 63-ФЗ и выдаваемая аккредитованным удостоверяющим центром; применяется для придания документам юридической силы во внешнем обороте. Технические и организационные условия применения УКЭП приведены в разделе А8.

1.5. **Ключ электронной подписи** — последовательность символов, предназначенная для создания подписи; **сертификат ключа проверки электронной подписи** (далее — «сертификат») — электронный документ, подтверждающий принадлежность ключа проверки владельцу.

1.6. **Заявка на выпуск** — оформленный Пользователем запрос на выпуск сертификата, указанный в Реестре (п. А3.6).

1.7. **Реестр сертификатов** — публичный общедоступный перечень выданных/отозванных сертификатов (серийный номер, отпечаток, статус, срок действия, вид/назначение) **без персональных данных**.

1.8. **Метка времени (TSA)** — штамп времени по протоколу RFC 3161, удостоверяющий момент формирования подписи или документа.

1.9. **Сервис «Подпись» не является:**

1.9.1. аккредитованным удостоверяющим центром по Закону № 63-ФЗ (до получения аккредитации) — в силу чего выпускаемые сертификаты имеют силу **внутри Экосистемы** и для отношений, где стороны признали такой порядок (см. А8); 1.9.2. стороной сделок, заключаемых Пользователями (см. А2).

А2. Роли сторон и правовое положение Оператора

2.1. Оператор — правообладатель программного обеспечения Сервиса «Подпись» и владелец УЦ Gramaton; он организует информационное взаимодействие и обеспечивает техническое функционирование УЦ.

2.2. Оператор **не является** стороной договоров, заключаемых между Пользователями, и не отвечает по их обязательствам, за исключением случаев, прямо предусмотренных законом и Соглашением.

2.3. Владельцем сертификата является Пользователь (физическое лицо, индивидуальный предприниматель или юридическое лицо), от имени которого выпущен сертификат. Ответственность за сохранность ключа электронной подписи, полученного Пользователем, и за действия, подписанные таким ключом, несёт владелец сертификата.

2.4. Участники взаимодействия (поставщики, исполнители, получатели, перевозчики, владельцы ПВЗ) используют подписи и сертификаты для подтверждения юридически значимых действий в Сервисах (подписание договоров, актов, накладных, отчётов, согласий, уведомлений).

А3. Порядок использования Сервиса

3.1. **Допуск к выпуску.** Сертификаты выпускаются Пользователям, прошедшим идентификацию (Приложение № 19 «Верификация»), а также по решению Оператора — доверенным доменам организации.

3.2. **Профили сертификатов.** УЦ выпускает сертификаты следующих назначений: физического лица, сотрудника организации, руководителя (единоличного исполнительного органа), корпоративного сертификата организации и сервисного сертификата (для автоматизированных интеграций). Назначение (профиль) сертификата определяет его допустимое использование.

3.3. **Способы выпуска.** Пользователь вправе: 3.3.1. сформировать ключ электронной подписи самостоятельно (ключ не покидает устройство Пользователя; УЦ выпускает сертификат на переданный открытый ключ); либо 3.3.2. использовать генерацию ключа на стороне УЦ, при этом ключ передаётся Пользователю один раз и хранится Оператором только в зашифрованном виде.

3.4. **Идентификация заявителя.** До выпуска сертификата заявитель проходит проверку (registration authority) — проверку документов Оператором, проверку через Сервис «Верификация», проверку по доверенному домену либо через внешние источники (ЕСИА/ЕГРЮЛ), если они подключены. Результат проверки фиксируется в журнале.

3.5. **Применение подписи.** Пользователь вправе подписывать документы и сообщения в Сервисах Экосистемы: договоры, акты, отчёты, заказы и заявки, передачу/приёмку товара, отчёты о доставке, согласия и уведомления. Подпись создаётся в формате, пригодном для проверки стандартными средствами (CMS/PKCS#7, CAdES-BES; для файлов PDF — встроенная подпись PAdES).

3.6. **Проверка и реестр.** Получатель и любое заинтересованное лицо вправе проверить подпись и статус сертификата. Для этого УЦ предоставляет: публичный реестр сертификатов, список отзыва сертификатов (CRL) и онлайн-проверку статуса (OCSP).

3.7. **Обязанности Пользователя.** Пользователь обязан: обеспечивать конфиденциальность ключа электронной подписи; не передавать ключ третьим лицам; незамедлительно уведомлять Оператора о подозрении на компрометацию ключа; предоставлять достоверные данные при выпуске.

3.8. **Запреты.** Не допускается: использование подписи для противоправных действий; выпуск сертификата на недостоверные данные; использование сертификата по назначению, не соответствующему его профилю; обход средств защиты УЦ.

3.9. **Приостановление и отзыв.** Оператор вправе приостановить действие сертификата (при подозрении на компрометацию) и отозвать его (по заявлению владельца, при прекращении полномочий, при нарушении настоящего Приложения, по законному требованию). Сведения об отзыве вносятся в CRL/OCSP. Приостановление может быть снято в порядке, определённом Оператором.

3.10. **Ограничение/приостановление доступа** к Сервису осуществляется по основаниям и в порядке, предусмотренным Соглашением (включая досудебное обжалование, раздел 15 Соглашения).

A4. Расчёты и вознаграждение

4.1. Использование Сервиса «Подпись» в базовом объёме (выпуск сертификатов участников Экосистемы и подписание документов в Сервисах) осуществляется без отдельной платы, если иное не установлено тарифами соответствующего Сервиса.

4.2. Оператор вправе устанавливать отдельную плату за расширенные (корпоративные, сервисные, высокообъёмные) режимы выпуска и сопровождения; тарифы публикуются на Сайте.

4.3. Расчёты по сделкам между Пользователями осуществляются в порядке соответствующего Приложения («Маркет», «Баланс взаиморасчётов») и не являются предметом настоящего Приложения.

A5. Споры и досудебный порядок

5.1. Споры, связанные с выпуском и использованием сертификатов, разрешаются в порядке раздела 9 Соглашения; досудебное обжалование — в порядке раздела 15 Соглашения.

5.2. Сторона, оспаривающая подпись, вправе запросить у Оператора сведения о статусе сертификата и сведения из журнала подписей в объёме, допустимом законом и Политикой.

А6. Ответственность и ограничения

6.1. Оператор отвечает за соответствие процедур УЦ настоящему Приложению и за сохранность приватных ключей УЦ. Оператор не отвечает за действия, подписанные ключом, находившимся во владении Пользователя, до момента уведомления о компрометации.

6.2. Пользователь несёт ответственность за достоверность данных, представленных при выпуске, и за правовые последствия использования своего сертификата.

6.3. Ограничения ответственности применяются в пределах, допускаемых законом, и не затрагивают права потребителя.

А7. Использование ЭП в Сервисах Экосистемы (в том числе «Маркет»)

7.1. **Общее правило.** Во всех Сервисах Экосистемы допускается использование ПЭП (для подтверждения действий Пользователя) и ЭП на сертификатах УЦ Gramaton (для подписания документов).

7.2. **Маркетплейс (gramaton.market).** 7.2.1. **Поставщики (продавцы, партнёры).** Для размещения Карточек Товаров и участия в расчётах Партнёр проходит проверку достоверности сведений (ч. 2 ст. 5 Закона № 289-ФЗ); результаты проверки, договор с Партнёром и юридически значимые документы (оферта-акцепт, акты, отчёты, уведомления) могут подписываться ЭП на сертификате УЦ Gramaton. 7.2.2. **Доставка, приёмка и передача Товара.** Подтверждение передачи/получения Заказа, приёмка Товара, акты передачи, действия по возвратам могут фиксироваться с электронной подписью участников (поставщика, перевозчика, владельца ПВЗ, получателя — в объёме, предусмотренном Приложением № 3 и Приложением № 12). 7.2.3. **Автоматизированные участники.** Для интеграций (склады, ПВЗ, перевозчики) могут выпускаться сервисные сертификаты; сервисы подписывают документы в автоматическом режиме.

7.3. **Иные Сервисы.** Аналогичный порядок применяется, соответственно, в «Подработке», «Такси», «CRM», «СЭД», «Бизнесе», «Кошельке/Балансе» и иных Сервисах — для подписания договоров, актов, сменных заданий, отчётов и юридически значимых сообщений.

7.4. **Юридически значимые сообщения.** Сообщения, подписанные ЭП и направленные через Сервисы (включая каналы Личного кабинета), считаются полученными надлежащим образом, если иное не установлено законом или конкретным Приложением; порядок и сроки определяются разделами 10 и 11 Соглашения.

А8. УКЭП, аккредитация и внешний оборот

8.1. Для применения **УКЭП** (п. 1.4.3) требуется использование средств криптографической защиты информации (СКЗИ), соответствующих требованиям законодательства, и **аккредитация удостоверяющего центра** в порядке Закона № 63-ФЗ. До завершения аккредитации УЦ Gramaton обеспечивает выпуск и применение ПЭП и ЭП на сертификатах УЦ Gramaton (УНЭП), а также подпись документов в форматах, проверяемых стандартными средствами.

8.2. Оператор развивает УЦ Gramaton как единую криптоинфраструктуру Экосистемы; после получения необходимых разрешений и подключения СКЗИ функциональность УКЭП вводится в действие без изменения настоящего Приложения (в части, не требующей правок) с публикацией обновления.

8.3. Документы, подписанные УКЭП в установленном порядке, признаются равнозначными документам на бумажном носителе, подписанным собственноручной подписью, в случаях и порядке, предусмотренных Законом № 63-ФЗ.

8.4. **Взаимное признание.** Стороны вправе в договорах между собой (в том числе в оферте Сервиса, акцептуемой Пользователем) признать юридическую силу подписей, сформированных УЦ Gramaton, в отношениях между этими сторонами (ст. 6, 9 Закона № 63-ФЗ — соглашение об использовании ЭП).

А9. Порядок изменения и версионирование

9.1. Настоящее Приложение изменяется в порядке раздела 10 Соглашения. Актуальная версия публикуется на Сайте (раздел «Документы» / «Подпись»).

ЧАСТЬ B. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

B1. Правовые основания обработки

- ст. 6 ч. 1 п. 5 152-ФЗ — обработка, необходимая для исполнения договора, стороной которого является субъект (выпуск и сопровождение сертификата, подписание и проверка документов);
- ст. 6 ч. 1 п. 2 152-ФЗ — обработка для осуществления прав и законных интересов Оператора (обеспечение информационной безопасности, предотвращение мошенничества), не нарушающих права субъекта;
- ст. 6 ч. 1 п. 1 152-ФЗ — при наличии согласия субъекта (в отдельных случаях верификации);
- отраслевые: 63-ФЗ (электронная подпись), 289-ФЗ (проверка партнёров маркетплейса).

B2. Категории персональных данных

- **Обычные:** фамилия, имя, отчество (или наименование), адрес электронной почты, контактный телефон, сведения о документе, удостоверяющем личность (в объёме, необходимом для идентификации), данные организации/ИП (наименование, ИНН, ОГРН/ОГРНИП, должность подписанта).
- **Технические (не ПД либо сведения ограниченного доступа):** открытый ключ, серийный номер и отпечаток сертификата, сведения о подписях (хэш подписанных данных, время, статус проверки).
- **Специальные (ст. 10 152-ФЗ):** не обрабатываются в рамках настоящего Приложения сверх объёма, определённого Приложением № 19 (при верификации документов).
- **Биометрические (ст. 11 152-ФЗ):** не обрабатываются в рамках настоящего Приложения.

B3. Субъекты и источники данных

- субъекты: Пользователи (физические лица, ИП, представители юридических лиц), подписанты;
- источники: сам субъект; Сервис «Верификация»; внешние источники (ЕСИА/ЕГРЮЛ), если подключены.

B4. Цели обработки (цель → данные → основание)

Цель	Состав данных	Основание
Идентификация заявителя и выпуск сертификата	ФИО/наименование, реквизиты, данные проверки документов	ст. 6 ч. 1 п. 5, п. 1 152-ФЗ; 63-ФЗ
Формирование и проверка электронной подписи	открытый ключ, серийный номер, отпечаток, хэш, время, статус	ст. 6 ч. 1 п. 5 152-ФЗ; 63-ФЗ
Ведение реестра и списка отзыва (CRL/OCSP)	серийный номер, отпечаток, статус, сроки	ст. 6 ч. 1 п. 2 152-ФЗ; 63-ФЗ
Обеспечение информационной безопасности и аудит	журналы операций, IP, метаданные событий	ст. 6 ч. 1 п. 2 152-ФЗ

B5. Сроки обработки и хранения

Данные	Срок	Основание	По истечении
Данные заявки на выпуск	до выпуска/отказа и далее в объёме, необходимом для подтверждения	ст. 5 152-ФЗ	удаление/обезличивание
Сведения о сертификате и подписях	срок действия сертификата + срок исковой давности	63-ФЗ, ГК РФ	удаление/архив
Журналы безопасности	до 6 месяцев (если иное не установлено)	ст. 6 ч. 1 п. 2 152-ФЗ	удаление

B6. Получатели и поручение обработки

- участники взаимодействия (получают необходимые сведения о сертификате/подписи для проверки);
- обрабоччики по поручению (ст. 6 ч. 3 152-ФЗ): поставщики инфраструктуры (ЦОД на территории РФ);
- госорганы — по законным запросам.

B7. Трансграничная передача

Не осуществляется. Хранение и обработка данных — на территории Российской Федерации (152-ФЗ, ст. 18 ч. 5). Передача за пределы РФ не производится.

B8. Меры защиты

- организационные (152-ФЗ ст. 18.1, ПП-1119); технические (Приказы ФСТЭК 17/21);
- криптографические меры (ФСТЭК-378): защита каналов, шифрование приватных ключей (AES-256-GCM), ключ шифрования вне базы данных;
- приватные ключи УЦ и участников хранятся **только в зашифрованном виде**; корневой ключ может выводиться в офлайн/HSM;
- разграничение доступа, журналирование (аудит-цепочка), резервное копирование в РФ.

B9. Права субъекта персональных данных

- права (гл. 3 152-ФЗ), в том числе доступ, уточнение, блокирование, уничтожение данных;
- порядок обращения: help@gramaton.pro; сроки ответа — в соответствии с законом и Политикой;
- отдельные права владельца сертификата (приостановление/отзыв) — раздел А3.9.

B10. Специфика Сервиса

10.1. Публичный реестр и CRL/OCSP содержат **только** метаданные сертификата (серийный номер, отпечаток, статус, сроки, вид) и **не содержат** персональных данных субъекта.

10.2. Приватные ключи участников, сгенерированные УЦ, хранятся в шифрованном виде и предоставляются владельцу однократно; Оператор не передаёт их третьим лицам.

10.3. Использование ЭП в рамках трудовых/подрядных отношений с участием работников партнёров осуществляется партнёром как самостоятельным оператором; Оператор обрабатывает данные только в объёме, необходимом для выпуска и проверки подписи.

Сводная таблица «данные × цель × основание × срок × получатель»

Данные	Цель	Основание	Срок	Получатель
ФИО/наименование, реквизиты, данные проверки	идентификация, выпуск сертификата	ст. 6 ч. 1 п. 5, п. 1 152-ФЗ; 63-ФЗ	до выпуска + срок подтверждения	УЦ (внутренне)
Открытый ключ, серийный номер, отпечаток, хэш, время, статус	формирование/проверка подписи	ст. 6 ч. 1 п. 5 152-ФЗ; 63-ФЗ	срок действия + срок исковой давности	участники взаимодействия
Серийный номер, отпечаток, статус, сроки	реестр, CRL/OCSP	ст. 6 ч. 1 п. 2 152-ФЗ; 63-ФЗ	срок действия сертификата	публично (без ПД)
Журналы операций, IP, метаданные	ИБ и аудит	ст. 6 ч. 1 п. 2 152-ФЗ	до 6 месяцев	УЦ (внутренне)