

ЧАСТЬ А. РЕГЛАМЕНТ СЕРВИСА

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

A1. Термины и определение Сервиса

1.1. **Сервис «Верификация»** — функциональный модуль Экосистемы Gramaton, обеспечивающий приём от Пользователя изображений документов, их распознавание и проверку уполномоченным лицом Оператора, формирование **персональной карты** Пользователя и **статуса верификации**, от которого зависит допуск Пользователя к отдельным функциям иных Сервисов Экосистемы (в частности, к отклику на заказы (смены) в Сервисе «Подработка» — Приложение № 1 и к принятию заказов в Сервисе «Такси» — Приложение № 2).

1.2. **Заявка** — комплект документов, загруженных Пользователем по выбранной категории, вместе с персональной картой, направленный на проверку.

1.3. **Категория (документальный статус, «работаю по»)** — одно из значений: *rf* — гражданин Российской Федерации; *vng* — работа по виду на жительство; *patent* — работа по патенту; *eaes* — граждане государств ЕАЭС (алиас *eaes* используется приложением в целях совместимости). Перечень документов, обязательных для каждой категории, является **единым и закрытым** и приведён в таблице ниже (п. 1.3.1–1.3.4).

1.3.1. Категория *rf* (гражданин РФ), все документы обязательны, по одной стороне: **паспорт; прописка; СНИЛС; ИНН.**

1.3.2. Категория *vng* (ВНЖ): **паспорт** (1 сторона); **ВНЖ (вид на жительство)** (2 стороны); **прописка; СНИЛС; ИНН.**

1.3.3. Категория *patent* (патент): **паспорт; миграционная карта** (2 стороны); **патент** (2 стороны); **карта иностранного гражданина** (2 стороны); **«зелёная карта»** (2 стороны); **полис ДМС; СНИЛС; ИНН; миграционный учёт** (в приложении отображается как «миграционный учёт / Амина»).

1.3.4. Категория *eaes* (страны ЕАЭС): **паспорт (карта)** (2 стороны); **миграционный учёт; СНИЛС; ИНН; карта иностранного гражданина** (2 стороны); **«зелёная карта»** (2 стороны).

1.4. **Документ (изображение документа)** — загруженное Пользователем изображение (фотография или скриншот) предъявленного документа, принимаемое в форматах JPEG, PNG или PDF с проверкой типа по содержимому файла и обязательной антивирусной проверкой (B8).

1.5. **Распознавание (OCR)** — автоматическое извлечение текста и отдельных полей из изображения документа средствами, работающими **на инфраструктуре Оператора** (без передачи изображений внешним сервисам). Результат распознавания носит **предварительный характер**, точность не гарантируется и **не является подтверждением подлинности** документа.

1.6. **Персональная карта** — структурированный набор сведений о Пользователе (в частности: ФИО, дата рождения, реквизиты документа, удостоверяющего личность, СНИЛС, ИНН, сроки действия документов), формируемый Пользователем, в том числе на основе результата распознавания, и сохраняемый в Сервисе. Заполнение карты не является обязательным условием отправки заявки на проверку, однако карта доступна проверяющему и используется при принятии решения.

1.7. **Статус верификации** — none (не пройдена / заявка не направлена), pending (на рассмотрении), verified (пройдена), rejected (отклонена). В контуре проверки дополнительно различаются промежуточные состояния заявки: **пересъёмка** (reshoot) и **эскалация** (escalated), а также состояние **обезличено** (anonymized, истечение срока хранения).

1.8. **Решение** — результат рассмотрения заявки уполномоченным лицом Оператора: одобрение, отклонение, направление на пересъёмку, эскалация. Отклонение и пересъёмка оформляются с указанием **причины из закрытого справочника** (например: признаки подделки; нечитаемое изображение; расхождение данных между документами; просроченный документ; не тот документ; неполный комплект; дубликат/повторная заявка после отказа; иное — с обязательным комментарием). Решение фиксируется в журнале решений и в журнале аудита (B6, B8).

1.9. **Сервис не является:** органом, удостоверяющим личность; оператором Единой системы идентификации и аутентификации (ЕСИА) или Единой биометрической системы (ЕБС); кредитной организацией; работодателем; перевозчиком; сервисом оценки кредитоспособности или платёжеспособности; органом, проводящим проверки, отнесённые законом к компетенции государственных органов.

1.10. **Результат Сервиса** (статус верификации, персональная карта) не является юридическим удостоверением личности, не заменяет документы, удостоверяющие личность, и не имеет силы сведений государственных информационных систем. Результат используется исключительно для целей допуска Пользователя к функциям Сервисов Экосистемы.

1.11. **Границы Сервиса.** Сервис не оформляет трудоустройство, не оказывает перевозки, не заключает договоры между Пользователями и не проводит проверку юридических лиц, индивидуальных предпринимателей и владельцев пунктов выдачи заказов (такие проверки относятся к иным контурам — Приложения № 12, 15, 16). Обработка персональных данных проверяющих Сервиса и кадрового контура панели проверки настоящим Приложением не регулируется.

1.12. **Пользователь** — дееспособное физическое лицо, имеющее Учётную запись Экосистемы Gramaton и акцептовавшее настоящее Приложение. Пользователь, направляющий заявку, далее также именуется **заявителем**.

1.13. Активация Сервиса (подача заявки) и его фактическое использование означают безусловный акцепт Пользователем настоящего Приложения (п. 3.3 Соглашения).

A2. Роли сторон и правовое положение Оператора

2.1. **Оператор** — правообладатель программного обеспечения Сервиса, владелец информационной инфраструктуры Экосистемы Gramaton, **оператор персональных данных** в смысле ст. 3 Закона № 152-ФЗ и организатор проверки документов.

2.2. Роль Оператора. Оператор принимает и хранит материалы, загруженные Пользователем, и организует их обработку. В объеме, в котором Сервис обеспечивает приём, хранение и техническую обработку материалов, загруженных Пользователем, Оператор действует в пределах, установленных ст. 1253.1 Гражданского кодекса РФ для информационного посредника: Оператор **не создаёт и не изменяет** содержание документов Пользователя. Вместе с тем, поскольку Оператор обязан проверить достоверность представленных Партнёром сведений до предоставления доступа к размещению или принятию заказов (ч. 2 ст. 5 Федерального закона от 31.07.2025 № 289-ФЗ), в этом объеме Оператор действует как **самостоятельно обязанное лицо** и отвечает за организацию проверки, а не только за техническую передачу материала. Окончательная правовая квалификация роли Оператора отнесена к открытым позициям (п. 2.4, 2.5).

2.3. Оператор не является: стороной отношений между Пользователем и Заказчиком (партнёром); работодателем; перевозчиком; продавцом товаров; исполнителем работ или услуг; кредитной организацией; оператором ЕСИА/ЕБС; лицом, выдающим официальные удостоверения личности.

2.4. О применимости Закона № 289-ФЗ. Сервис сам по себе не является посреднической цифровой платформой в смысле Закона № 289-ФЗ, поскольку не обеспечивает реализацию товаров, работ или услуг, предлагаемых партнёрами. Сервис обеспечивает функцию подтверждения личности, которая используется платформенными Сервисами Экосистемы (в частности, «Подработка», «Такси»). Независимо от правовой квалификации Сервиса Оператор **добровольно применяет** следующие принципы, соответствующие ст. 13–14 Закона № 289-ФЗ: ограничение допуска — только по закрытому перечню оснований (п. А3.7); мотивированное уведомление Пользователя (п. А3.9); право Пользователя на досудебное обжалование (п. А5); отмена меры при признании жалобы обоснованной (п. А5.3); сохранение доступа к Личному кабинету при ограничении отдельных функций (ч. 4 ст. 13 Закона № 289-ФЗ; п. А3.8).

2.5. Ограничение ответственности Оператора за решения третьих лиц. Оператор не отвечает за решения Заказчиков (партнёров) и иных Пользователей, принимаемые с учётом статуса верификации, и за их последствия, за исключением обязательств, прямо принятых на себя по настоящему Приложению и Соглашению.

2.6. **Пользователь** обязуется: загружать **только собственные** документы; не загружать поддельные, изменённые, чужие или недействительные документы; предоставлять достоверные сведения; не передавать доступ к Учётной записи третьим лицам.

2.7. **Права третьих лиц.** Ответственность за правомерность загрузки документов, содержащих сведения третьих лиц (если такие документы предъявляются), несёт Пользователь, загрузивший их. Оператор вправе не рассматривать такую заявку и применить меры по п. А3.7.

А3. Порядок использования Сервиса

3.1. **Доступ.** Использование Сервиса осуществляется через единую Учётную запись Экосистемы Gramaton; отдельная регистрация в Сервисе не требуется. Аутентификация выполняется по токену доступа, выдаваемому сервисом аутентификации Экосистемы (проверяются подпись, срок действия, издатель, получатель). Уполномоченные лица Оператора работают в закрытой панели проверки: вход — по учётным данным панели с обязательной многофакторной аутентификацией (пароль + одноразовый код), сессии короткие (30 минут) и криптографически подписаны; доступ ограничивается по сетевому разрешению (IP-allowlist) и по служебному токену единого входа (B8).

3.2. **Выбор категории.** Пользователь выбирает категорию (п. 1.3), которой соответствует перечень обязательных документов. Изменение категории влечёт изменение состава обязательных документов.

3.3. **Загрузка документов.** Пользователь загружает изображения обязательных документов, выбирая источник «камера / галерея» (скриншоты допустимы). Для каждого документа может быть загружено от одной до двух сторон (в зависимости от документа, п. 1.3.1–1.3.4). Принимаются файлы JPEG, PNG и PDF; тип файла проверяется по содержимому, а не по расширению; размер файла ограничен; каждый файл проходит антивирусную проверку до предоставления доступа к нему (B8).

3.4. **Распознавание и подтверждение полей.** После загрузки документа Оператор выполняет распознавание текста на своей инфраструктуре; результат отображается Пользователю (распознанный текст и извлечённые поля) с возможностью **подтвердить или исправить** значения. Подтверждённые значения применяются к персональной карте Пользователя. Результат распознавания не является проверкой подлинности документа и не заменяет решение уполномоченного лица (п. А1.5, А1.8).

3.5. Направление заявки на проверку. Пользователь направляет заявку на проверку. Если комплект неполон, заявка не принимается, а Пользователю сообщается перечень недостающих документов. Пользователь также вправе очистить ранее загруженные материалы («Пройти заново» / «Сбросить и переснять») и загрузить их повторно.

3.6. Рассмотрение заявки. Заявку рассматривает уполномоченное лицо Оператора, обладающее соответствующим правом доступа. По умолчанию сведения о Пользователе отображаются проверяющему **в маскированном виде**; раскрытие персональных данных (просмотр в открытом виде) возможно только для роли, наделённой таким правом, и **с обязательным указанием причины** раскрытия. Факты просмотра и раскрытия персональных данных фиксируются в журнале аудита. Пересмотр ранее принятого решения другим сотрудником требует дополнительного права (принцип «четырёх глаз»).

3.7. Основания ограничения допуска (закрытый перечень). Оператор отказывает в предоставлении допуска к функциям, требующим подтверждённой личности, только в следующих случаях:

3.7.1. представление недостоверных документов, документов с признаками подделки или изменения; 3.7.2. нечитаемое изображение документа либо невозможность прочтения существенных реквизитов (направляется на пересъёмку); 3.7.3. расхождение сведений между предъявленными документами либо с данными Учётной записи; 3.7.4. предъявление документа с истёкшим сроком действия; 3.7.5. предъявление не того документа, который требуется для выбранной категории, либо непредставление полного комплекта обязательных документов; 3.7.6. повторная заявка после отказа, не содержащая новых сведений (дубликат); 3.7.7. непредставление документов, обязательных в силу законодательства Российской Федерации для соответствующего вида деятельности, в объёме, необходимом для допуска; 3.7.8. поступление требования (предписания) уполномоченного государственного органа в случаях, предусмотренных законом; 3.7.9. невозможность установить соответствие данных заявителя предъявленным документам имеющимися средствами проверки.

3.8. Последствия ограничения. До получения статуса «пройдена» Оператор отказывает Пользователю в совершении действий, требующих подтверждённой личности: в отклике на заказ (смену) в Сервисе «Подработка» и в принятии заказа в Сервисе «Такси». Пользователю выводится единое сообщение о необходимости пройти идентификацию документов (раздел «Профиль → Верификация»). Доступ к Учётной записи и к иным Сервисам Экосистемы при этом **не ограничивается**; доступ к Личному кабинету не блокируется (ч. 4 ст. 13 Закона № 289-ФЗ).

3.9. Уведомление и повторная подача. Пользователь видит актуальный статус заявки, а при отклонении — причину. Отклонение не лишает Пользователя права на повторную подачу документов (после устранения причины), на пересъёмку и на обжалование (п. А5). При ограничении допуска Оператор направляет мотивированное уведомление с указанием основания и порядка обжалования.

3.10. Техническая доступность реестра статусов. Проверка статуса выполняется Сервисами Экосистемы автоматически при совершении соответствующего действия. Если реестр статусов технически недоступен (сбой, таймаут, отсутствие ответа), Сервисы могут **не применять** ограничение — в целях непрерывности работы Экосистемы. Оператор не гарантирует, что в период технической недоступности функции будут ограничены; такие случаи отражаются в технических журналах.

3.11. Обязанности Пользователя: загружать достоверные документы, принадлежащие самому Пользователю; не искажать сведения; не загружать документы третьих лиц без законного основания; незамедлительно уведомлять Оператора о выявлении недостоверности ранее поданных сведений; не предпринимать попыток обхода порядка проверки (в том числе автоматизированными средствами). Порядок и срок уведомления об изменении сведений, влияющих на допуск (по аналогии с п. 12.6 Соглашения — не позднее 3 (трёх) рабочих дней), для заявителя отнесён к открытым позициям.

3.12. Права Пользователя: подать заявку и загрузить документы; получить информацию о статусе и причине отказа; исправить персональную карту; очистить загруженные материалы и подать заявку повторно; направить обращение (жалобу) и обжаловать решение в досудебном порядке (п. А5); отозвать согласие на обработку персональных данных (здесь и далее — «ПД») и реализовать права субъекта ПД (В9).

3.13. **Изменение условий** настоящего Приложения осуществляется с соблюдением сроков уведомления, установленных п. 10.3 Соглашения (45 (сорок пять) календарных дней — для изменений тарифов, ответственности и условий выполнения заказов; 15 (пятнадцать) календарных дней — для прочих изменений; ст. 12 Закона № 289-ФЗ).

A4. Расчёты, вознаграждение, возвраты

4.1. Использование Сервиса «Верификация» для Пользователя является **бесплатным**; плата за проверку документов Оператором не взимается, вознаграждение за проверку не устанавливается.

4.2. Расчёты между Пользователем и Оператором в рамках Сервиса **не осуществляются**: Оператор не принимает и не перечисляет денежные средства в связи с верификацией, обеспечительные платежи в Сервисе не применяются.

4.3. Платные функции Сервиса (в том числе приоритетная (ускоренная) проверка, платная повторная проверка, платное раскрытие результата) на дату настоящей редакции **не реализованы**; списания денежных средств не производятся. При введении таких функций: состав, стоимость и порядок оплаты раскрываются Оператором до совершения оплаты; при расчётах формируются чеки в соответствии с законодательством Российской Федерации; порядок возврата определяется законом и Соглашением; права Пользователя как потребителя, установленные Законом РФ «О защите прав потребителей», не ограничиваются.

4.4. Доход от Сервиса Оператором не формируется. Условия расчётов между Пользователями и Заказчиками (партнёрами) настоящим Приложением не регулируются и определяются приложениями соответствующих Сервисов (в частности, Приложениями № 1, 2, 5).

4.5. **Реклама и рассылки.** Рекламные и маркетинговые сообщения направляются Пользователям только при наличии отдельного согласия (ст. 18 Федерального закона «О рекламе»). В рамках Сервиса «Верификация» рекламные и маркетинговые сообщения не направляются; таргетирование рекламы на основе данных верификации не осуществляется.

A5. Споры, обращения и досудебное обжалование

5.1. Обращения и жалобы направляются через форму обратной связи в приложении (Личный кабинет) либо по адресу электронной почты Оператора **help@gramaton.pro**.

5.2. Сроки рассмотрения:

5.2.1. жалоба на ограничение допуска (отказ по заявке, направление на пересъёмку) — не более 15 (пятнадцати) календарных дней со дня регистрации жалобы, в порядке раздела 15 Соглашения (ч. 2 ст. 14 Закона № 289-ФЗ); 5.2.2. обращения Пользователя как субъекта ПД (в том числе об уточнении, блокировании, уничтожении ПД, об отзыве согласия) — не более 10 (десяти) рабочих дней со дня получения обращения; срок может быть продлён не более чем на 5 (пять) рабочих дней с направлением мотивированного уведомления (ч. 1 ст. 20 Закона № 152-ФЗ); 5.2.3. иные обращения — в срок, установленный разделом 15 Соглашения.

5.3. **Отмена меры.** При признании жалобы обоснованной применённая мера (отказ в допуске) отменяется в течение 48 (сорока восьми) часов со дня принятия решения по жалобе (ч. 3 ст. 13, ч. 3 ст. 14 Закона № 289-ФЗ). Факт отмены отражается в журнале решений и в журнале аудита.

5.4. Ответ на жалобу оформляется мотивированно, с указанием установленных обстоятельств, применённых норм и выводов, и направляется заявителю через Личный кабинет и (или) по каналам юридически значимых сообщений. Жалоба рассматривается подразделением (специалистом), не участвовавшим в принятии обжалуемого решения (п. 15.9 Соглашения).

5.5. Журнал жалоб ведётся с фиксацией даты подачи, даты регистрации, даты решения, результата и применённых мер (п. 15.8 Соглашения).

5.6. До обращения в суд по имущественным и договорным спорам соблюдается обязательный претензионный порядок: срок ответа на претензию — 30 (тридцать) календарных дней, если иной срок не установлен законом (п. 9.3 Соглашения). Право субъекта ПД на обращение в Роскомнадзор или в суд не ограничивается (B9).

А6. Ответственность и ограничения

6.1. Сервис предоставляется «как есть» (as is). Оператор не гарантирует бесперебойную и безошибочную работу Сервиса, бесперебойную работу распознавания документов, а также точность распознавания; Оператор принимает разумные меры для поддержания работоспособности Сервиса.

6.2. Оператор **не несёт ответственности** за: содержание и достоверность документов, представленных Пользователем; последствия представления недостоверных, поддельных или чужих документов; решения Заказчиков (партнёров) и иных Пользователей, принимаемые с учётом статуса верификации; действия третьих лиц и государственных органов; обстоятельства непреодолимой силы.

6.3. Ограничения ответственности, установленные Соглашением и настоящим Приложением, **не применяются** к правам потребителя, установленным Законом РФ «О защите прав потребителей», и к ответственности за вред жизни и здоровью. Ответственность Оператора в объёме, в котором он действует как информационный посредник, определяется с учётом ст. 1253.1 ГК РФ.

6.4. Результат Сервиса не является официальным подтверждением личности и не порождает для третьих лиц обязанности признавать личность Пользователя установленной. Оператор не отвечает за отказ третьих лиц (включая государственные органы, банки, работодателей) признать результат Сервиса.

6.5. Оператор принимает меры по ограничению доступа к информации, распространение которой запрещено, по требованиям уполномоченных органов в порядке, установленном Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

ЧАСТЬ В. ОСОБЕННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

В1. Правовые основания обработки

• **ст. 6 ч. 1 п. 1 Закона № 152-ФЗ** — согласие субъекта ПД: подача заявки, загрузка документов, распознавание, формирование и корректировка персональной карты, проверка уполномоченным лицом, хранение копий документов, обработка специальных категорий ПД в объеме, следующем из предъявленных документов (в совокупности со ст. 10 ч. 2 п. 1). В Экосистеме предусмотрен журнал согласий, в котором фиксируются документ (terms — Пользовательское соглашение, privacy — Политика), версия документа, дата и время, IP-адрес и пользовательский агент. - **ст. 6 ч. 1 п. 5 Закона № 152-ФЗ** — исполнение договора, стороной которого является субъект ПД (Соглашение и настоящее Приложение): предоставление доступа к функциям Сервисов Экосистемы, передача статуса верификации в Сервисы «Подработка» и «Такси», формирование персональной карты, рассмотрение обращений. - **ст. 6 ч. 1 п. 2 Закона № 152-ФЗ** — исполнение обязанностей, возложенных на Оператора законодательством РФ: Закон № 152-ФЗ (реализация прав субъектов, ответы на обращения, уничтожение ПД, уведомление Роскомнадзора, обеспечение безопасности); ч. 2 ст. 5 Закона № 289-ФЗ (проверка достоверности представленных Партнёром сведений до предоставления доступа к размещению или принятию заказов); Закон № 149-ФЗ; Закон № 115-ФЗ — в объеме, применимом к Оператору в рамках внутреннего контроля в целях ПОД/ФТ (Приложение № 11); исполнение мотивированных запросов уполномоченных государственных органов, включая Федеральный закон от 06.07.2016 № 374-ФЗ (в применимой части). - **ст. 6 ч. 1 п. 4 Закона № 152-ФЗ** — защита жизни, здоровья и иных жизненно важных интересов субъекта ПД (применяется в исключительных случаях; - **ст. 9 Закона № 152-ФЗ** — требования к согласию, включая сведения, предусмотренные ч. 4 ст. 9; согласие оформляется отдельно от иных документов и не может быть «зашито» в текст оферты. - **ст. 10 ч. 2 п. 1 Закона № 152-ФЗ** — обработка специальных категорий ПД допускается при наличии письменного согласия субъекта (состав данных — В2, В10). - **ст. 11 Закона № 152-ФЗ** — биометрические ПД: **не обрабатываются** (решение Оператора от 29.09.2026; В2, В10). - **ст. 12 Закона № 152-ФЗ** — трансграничная передача ПД не осуществляется (В7). - **ст. 18 ч. 5 Закона № 152-ФЗ** — обработка ПД граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации. - **ст. 22 Закона № 152-ФЗ** — уведомление Роскомнадзора об обработке ПД (уведомление подготовлено; факт подачи — организационная позиция Оператора). - **Федеральный закон от 06.04.2011 № 63-ФЗ** — на дату редакции электронная подпись в Сервисе **не применяется**: решения и статусы формируются в информационной системе Оператора, а

юридически значимый электронный документооборот обеспечивается иным Сервисом Экосистемы (Приложение № 14).

Требования постановления Правительства РФ от 01.11.2012 № 1119, приказов ФСТЭК России № 21 и № 378 являются требованиями к **защите** ПД, а не самостоятельными основаниями обработки (см. В8).

В2. Категории персональных данных

Обычные персональные данные (обрабатываются по факту):

- идентификатор Учётной записи Экосистемы (`uuid`) и признак принадлежности к категории документального статуса (`rf`, `vng`, `patent`, `eaes`);
- фамилия, имя, отчество (при наличии); дата и место рождения; пол; гражданство;
- данные документа, удостоверяющего личность: вид документа, серия и номер, дата выдачи, орган выдачи, срок действия;
- реквизиты иных предъявленных документов: прописка (регистрация), СНИЛС, ИНН, полис ДМС, миграционная карта, патент, вид на жительство (ВНЖ/РВП), карта иностранного гражданина, «зелёная карта», миграционный учёт;
- изображения предъявленных документов (фотографии и скриншоты, до двух сторон одного документа);
- текст, распознанный автоматизированными средствами (`raw_text`), и извлечённые поля (`extracted`, перечень полей зависит от типа документа);
- персональная карта Пользователя (структурированный набор подтверждённых полей);
- статус верификации, статус документов, решения и причины решений, сигналы риска (например: признаки подделки, нечитаемое изображение, расхождение данных, документ с истёкшим сроком, вероятный дубликат);
- контактные данные Учётной записи (номер мобильного телефона, адрес электронной почты) — обрабатываются в единой Учётной записи Экосистемы; передаются в реестр статусов в объёме, необходимом для сопоставления заявки, а также используются для служебных уведомлений;
- технические данные обращения к Сервису: IP-адрес, тип устройства и браузера (`user-agent`), данные сессии (`cookie` и `session` в панели проверки);
- метаданные файлов документов: контрольная сумма (`sha256`), размер, MIME-тип, результат антивирусной проверки, идентификатор объекта в хранилище;

- журналы аудита панели проверки: входы и выходы, неуспешные входы, смена пароля, отказы доступа, решения, просмотр и раскрытие ПД, экспорт доказательств;
- **служебные ПД уполномоченных лиц Оператора:** учётная запись панели (логин), роль, хеш пароля, секрет двухфакторной аутентификации, действия в системе.

Специальные категории (ст. 10 Закона № 152-ФЗ): Оператор **целенаправленно не запрашивает** специальные категории ПД. Вместе с тем из предъявленных документов объективно следуют сведения:

- раскрывающие гражданство и национальную принадлежность (паспорт гражданина РФ, паспорт иностранного гражданина, миграционные документы);
- относящиеся к состоянию здоровья — **только в объёме, содержащемся в предъявленных документах** (например, отметки и справки, полис ДМС);
- сведения о судимости — **только если соответствующий документ предъявлен субъектом добровольно.**

Обработка таких сведений допускается при наличии **письменного согласия субъекта** (ст. 10 ч. 2 п. 1 Закона № 152-ФЗ) и ограничивается целями верификации.

Биометрические персональные данные (ст. 11 Закона № 152-ФЗ): не обрабатываются. Изображение лица (селфи) не запрашивается и не хранится; сличение изображения лица с фотографией в документе автоматизированными средствами не производится; формирование биометрических шаблонов, биометрическая идентификация и аутентификация не осуществляются; средства распознавания лиц не применяются и не подключаются (решение Оператора от 29.09.2026). Ранее загруженные изображения лица (в тестовых заявках) удалены. См. также B10.

Иные данные: факты согласий (документ, версия, дата и время, IP-адрес, user-agent); обращения, жалобы и материалы их рассмотрения; сведения о решениях по жалобам.

Геолокация: координаты местоположения в Сервисе не обрабатываются.

B3. Субъекты и источники данных

- **Субъекты:** Пользователи, направившие заявку на верификацию (граждане Российской Федерации, граждане государств ЕАЭС, иные иностранные граждане и лица без гражданства, работающие по виду на жительство или патенту); Пользователи, направившие обращение (жалобу); уполномоченные лица Оператора — в части служебных ПД.

- **Источники:** сам субъект (загрузка документов, заполнение и корректировка персональной карты, действия в Сервисе, обращения); единая Учётная запись Экосистемы Gramaton (идентификатор Пользователя, контактные данные) — получение по защищённому внутреннему каналу; технические журналы Сервиса и панели проверки (формируются автоматически); уполномоченные государственные органы (требования, предписания, мотивированные запросы).
- Ответственность за достоверность и правомерность загруженных документов, а также за правомерность предъявления документов, содержащих сведения третьих лиц, несёт Пользователь.

В4. Цели обработки (цель → данные → основание)

№	Цель обработки	Состав данных	Правовое основание
1	Идентификация заявителя; проверка подлинности документов, удостоверяющих личность, и соответствия данных заявителя предъявленным документам	ФИО, дата и место рождения, пол, гражданство; реквизиты документов; изображения документов; результат распознавания	ст. 6 ч. 1 п. 1; ст. 9; для специальных категорий — ст. 10 ч. 2 п. 1
2	Формирование, корректировка и хранение персональной карты Пользователя	подтверждённые поля карты; результат распознавания	ст. 6 ч. 1 п. 1, п. 5
3	Принятие решения по заявке (одобрение, отклонение, пересъёмка, эскалация) и информирование заявителя о статусе и причине	статус, решение, причина решения, сигналы риска; служебные данные проверяющего	ст. 6 ч. 1 п. 1, п. 5
4	Предоставление допуска к функциям Сервисов Экосистемы, требующим подтверждённой личности («Подработка», «Такси»)	статус верификации, признак категории, статус документов	ст. 6 ч. 1 п. 5; ч. 2 ст. 5 Закона № 289-ФЗ
5	Внутренний учёт заявок, аудит действий, обеспечение информационной безопасности, предотвращение мо-	метаданные файлов, журналы аудита, сигналы риска, технические данные	ст. 6 ч. 1 п. 2, п. 5 (в пределах, допускаемых законом)

№	Цель обработки	Состав данных	Правовое основание
	шенничества (дубликаты, подделки, повторные заявки)		
6	Управление доступом уполномоченных лиц Оператора, служебный учёт их учётных записей и действий	учётные данные панели, роль, журнал аудита, IP-адрес	ст. 6 ч. 1 п. 2; ст. 18.1, 19
7	Рассмотрение обращений (жалоб), реализация прав субъекта ПД, досудебное обжалование	обращение, идентификатор Пользователя, контактные данные, материалы рассмотрения	ст. 6 ч. 1 п. 1, п. 2
8	Исполнение требований законодательства РФ, в том числе предоставление информации уполномоченным органам	данные в объёме мотивированного запроса (требования)	ст. 6 ч. 1 п. 2
9	Обеспечение непрерывности работы и восстановления данных (резервное копирование, восстановление)	данные в объёме резервных копий	ст. 6 ч. 1 п. 2, п. 5
10	Защита жизни, здоровья и иных жизненно важных интересов субъекта (исключительные случаи)	данные, необходимые для реагирования	ст. 6 ч. 1 п. 4

Обработка ПД ограничивается конкретными, заранее определёнными и законными целями; «резервные» цели не устанавливаются (ст. 5 Закона № 152-ФЗ). Объединение баз данных, обработка которых осуществляется в целях, несовместимых между собой, не допускается. Профилирование Пользователей для целей рекламы не осуществляется; данные верификации в коммерческих целях не используются.

В5. Сроки обработки и хранения

Данные	Срок	Основание / порядок
Изображения документов (в контуре панели проверки)	до истечения срока хранения, определяемого итоговым статусом заявки: одобренные — 5 (пять) лет ; отклонённые, направ-	цель проверки, подтверждение решения, защита от повторного

Данные	Срок	Основание / порядок
	ленные на пересъёмку, эскалированные — 1 (один) год (от даты решения); далее — обезличивание	мошенничества; Политика (раздел 6)
Запись о заявке, решение, причина решения, сигналы риска (в обезличенном виде)	сохраняются после обезличивания как метаданные (для отчётности)	Политика (раздел 6)
Персональная карта, записи о документах и файлы документов в контуре реестра статусов	до удаления Учётной записи Пользователя (при удалении Учётной записи записи о документах, персональная карта и файлы документов удаляются)	ст. 21 Закона № 152-ФЗ; требование к удалению аккаунта по инициативе Пользователя
Журнал аудита действий	3 (три) года	внутренний контроль и информационная безопасность; Политика (раздел 6)
Технические журналы, IP-адрес, user-agent, данные сессии	1 (один) год	Политика (раздел 6)
Служебные учётные записи уполномоченных лиц	до прекращения полномочий (отключения учётной записи) + срок хранения журналов аудита	ст. 18.1, 19 Закона № 152-ФЗ
Данные, обработка которых велась на основании согласия	до отзыва согласия, но не более срока цели	ст. 21 Закона № 152-ФЗ
Факты согласий (документ, версия, дата, IP, user-agent)	срок использования Учётной записи + 3 (три) года	подтверждение заключения договора и согласий

5.1. По истечении срока хранения ПД подлежат уничтожению или обезличиванию в порядке, предусмотренном ст. 21 Закона № 152-ФЗ и локальными актами Оператора; факт уничтожения (обезличивания) фиксируется в журнале с указанием перечня данных и способа.

5.2. **Реализованный порядок обезличивания.** В контуре панели проверки заявка после принятия решения переводится в защищённый режим с установлением срока хранения; по истечении срока структурированные ПД заявки заменяются обезличенной заглушкой, статус заявки изменяется на «обезличено», а действие фиксируется в журнале аудита. **Ограничение:** указанный порядок обезличивает структурированные сведения, но **не удаляет сами файлы изображений документов и записи о документах** в объектном хранилище;

5.3. **Сроки в контуре реестра статусов.** Автоматическое удаление или обезличивание заявок по истечении срока хранения в контуре реестра статусов на дату редакции **не реализовано:** данные удаляются при удалении Учётной записи Пользователя.

5.4. **Расхождение ориентиров сроков.** Политика (раздел 6) содержит иные ориентиры сроков (в частности: изображения документов — 12 (двенадцать) месяцев после принятия решения; запись о заявке и решении — 3 (три) года; журнал аудита — 3 (три) года) и указывает, что конкретные сроки подлежат утверждению Оператором. До утверждения единого порядка применяется принцип «не дольше, чем требуется целями обработки»;

5.5. При отзыве согласия Оператор прекращает обработку и уничтожает ПД в срок, не превышающий 30 (тридцати) дней (ч. 5 ст. 21 Закона № 152-ФЗ), за исключением данных, обработка которых может быть продолжена на ином законном основании (например, сведения о принятом решении и о фактах противоправных действий — для защиты от повторного мошенничества и подтверждения решения).

В6. Получатели и поручение обработки

- **Уполномоченные лица Оператора** (роли контура верификации: наблюдатель, верификатор уровня L1, верификатор уровня L2, комплаенс-лид, аудитор, администратор, ответственный за ПД) — доступ по принципу минимальных привилегий; по умолчанию ПД отображаются маскированно; раскрытие — только для роли, наделённой правом, и с обязательной причиной (фиксируется в журнале аудита); пересмотр чужого решения — по принципу «четырёх глаз». - **Сервисы Экосистемы Gramaton, использующие результат верификации:** «Подработка» (отклик на заказы (смены)) и «Такси» (принятие заказов). Передаётся **только статус верификации (и признак статуса документов)** по защищённому внутреннему запросу; содержание документов, персональная карта и результаты распознавания в эти Сервисы **не передаются**. - **Сервис аутентификации и единой Учётной записи Экосистемы** — идентификация Пользователя и уполномоченных лиц Оператора (служебный токен единого входа). - **Лица, привлечённые к обработке по поручению** (ч. 3 ст. 6 Закона № 152-ФЗ): поставщики инфраструктуры и центров обработки данных на территории Российской Федерации; сервис объектного хранилища; средства антивирусной проверки; оператор связи (доставка служебных уведомлений); служба поддержки. Обработка осуществляется на основании договоров, содержащих обязательства о конфиденциальности и безопасности ПД; - **Государственные органы** (Роскомнадзор, МВД, ФСБ, суды, органы прокуратуры) — по мотивированным запросам (требованиям) в случаях и порядке, установленных законодательством РФ. - **Иные получатели.** В коммерческих целях ПД третьим лицам **не передаются**. Банкам-партнёрам и операторам платёжной инфраструктуры данные верификации не передаются (расчёты регулируются иными приложениями); передача сведений в рамках внутреннего контроля в целях ПОД/ФТ осуществляется в порядке Приложения № 11. Работодателям, Заказчикам (партнёрам) и иным Пользователям сведения о верификации не раскрываются — им доступен только результат в объёме функциональной возможности соответствующего Сервиса.

В7. Трансграничная передача

7.1. Трансграничная передача персональных данных в рамках Сервиса

«Верификация» Оператором **не осуществляется**. Обработка, запись, систематизация, накопление, хранение, уточнение (обновление, изменение) и извлечение ПД граждан Российской Федерации осуществляются с использованием баз данных, находящихся на территории Российской Федерации (ч. 5 ст. 18 Закона № 152-ФЗ). Резервные копии размещаются также на территории Российской Федерации.

7.2. Действующие редакции Соглашения (п. 1.9.1–1.9.2) и Политики (раздел 7) содержат положения о трансграничной передаче ПД на территорию иностранных государств (Королевство Нидерландов; Федеративная Республика Германия — при необходимости) в целях обеспечения отказоустойчивости и резервного копирования. **Расхождение** между указанными положениями и фактическим порядком обработки (локализация на территории Российской Федерации) подлежит устранению в порядке, предусмотренном внутренним планом Оператора. В настоящем Приложении использована формулировка, соответствующая фактическому порядку обработки и уведомлению об обработке ПД; существующие документы настоящим Приложением не изменяются. Позиция отнесена к открытым.

7.3. Любое изменение порядка, указанного в п. 7.1, возможно только после выполнения требований ст. 12 Закона № 152-ФЗ (включая, при необходимости, получение согласий субъектов и уведомление Роскомнадзора) и внесения соответствующих изменений в Политику и Соглашение.

В8. Меры защиты персональных данных

Организационные меры (ст. 18.1, 19 Закона № 152-ФЗ; постановление Правительства РФ от 01.11.2012 № 1119):

- назначение лица, ответственного за организацию обработки ПД (приказ № 1-ПД от 29.09.2026 — черновик, подлежит подписанию);
- утверждение Политики обработки ПД, правил обработки и обезличивания ПД, перечня информационных систем персональных данных (ИСПДн) с уровнем защищённости **УЗ-2** и порядка допуска лиц к обработке ПД (документы подготовлены, подлежат утверждению);

- определение информационной системы Сервиса как ИСПДн «Подсистема верификации документов (KYC)» с расчётным уровнем защищённости УЗ-2;
- внутренний контроль соответствия обработки требованиям законодательства; ознакомление допущенных лиц с документами и проведение инструктажей;
- регламент реагирования на инциденты, включая уведомление Роскомнадзора о факте инцидента в течение 24 часов и о результатах расследования — в течение 72 часов (ч. 3.1 ст. 21 Закона № 152-ФЗ);
- порядок уничтожения ПД и фиксации фактов уничтожения (ст. 21 Закона № 152-ФЗ);
- уведомление Роскомнадзора об обработке ПД (ст. 22 Закона № 152-ФЗ).

Технические и программные меры (базовый набор мер для УЗ-2, приказ ФСТЭК России от 18.02.2013 № 21):

- **ИАФ** — идентификация и аутентификация: проверка токенов доступа (подпись, срок действия, издатель, получатель); для уполномоченных лиц — пароль в зашифрованном виде, обязательная двухфакторная аутентификация (одноразовые коды), короткие сессии (30 минут) с криптографической подписью, ограничение числа попыток входа (10 попыток за 15 минут), сетевое ограничение доступа к панели (IP-allowlist), служебный токен единого входа; - **УПД** — управление доступом: ролевая модель с разграничением прав по доменам (верификация, кадры, безопасность, выплаты, администрирование и аудит); принцип минимальных привилегий; маскирование ПД по умолчанию; обязательная причина раскрытия ПД; принцип «четырёх глаз» при рассмотрении решения; критические операции выделены и контролируются; - **РСБ** — регистрация событий безопасности: журнал аудита фиксирует входы и выходы, неуспешные входы, смену пароля, отказы доступа, решения, просмотр и раскрытие ПД (с причиной), экспорт доказательств, обезличивание; - **ОПС / УКФ** — ограничение программной среды и управление конфигурацией: размещение Сервиса и панели проверки в изолированных контейнерах, доступ только через защищённый обратный прокси, служебные порты открыты только локально; - **ЗНИ / ЗИС** — защита носителей и каналов: шифрование персональных данных в покое (AES-256-GCM) в контуре панели проверки с хранением ключа вне базы данных и возможностью ротации ключей; защита каналов передачи (TLS, HSTS, политика безопасности содержимого, запрет встраивания и подмены MIME-типа); файлы документов хранятся в **защищённом каталоге**, не в публичной статике, и выдаются только по подписанной ссылке с коротким сроком действия и проверкой подписи; - **АНЗ** — антивирусная защита: каждый загружаемый файл проверяется до предоставления доступа к нему; при недоступности базы сигнатур файл **не выдаётся** (fail-closed); дополнительно контролируется фактический тип файла по содержимому и ограничивается размер файла; - **СОВ** — обнаружение вторжений и защита периметра: автоматическая блокировка сканеров и ботов, закрытые служебные порты, контроль внешнего периметра; - **ОДТ** — доступность: ежедневное резервное копирование (в том числе томов панели проверки), резервные копии с шифрованием, контроль восстановления; - размещение баз данных, содержащих ПД граждан Российской Федерации, на территории Российской Федерации (ч. 5 ст. 18 Закона № 152-ФЗ).

Криптографические меры: применяются в случаях, предусмотренных законодательством РФ, в соответствии с приказом ФСТЭК России от 10.04.2025 № 378. Класс средств криптографической защиты информации на дату редакции **не определён**;

Оговорка о статусе. Уровень защищённости УЗ-2 является расчётным (постановление Правительства РФ № 1119). Аттестация информационной системы персональных данных не проводилась. Документы по организационным мерам подлежат утверждению Оператором.

В9. Права субъекта персональных данных

9.1. Субъект ПД имеет право: получать информацию, касающуюся обработки его ПД (ст. 14 Закона № 152-ФЗ); требовать уточнения ПД, их блокирования или уничтожения, если они неполны, устарели, неточны, получены незаконно или не являются необходимыми для заявленной цели обработки (ст. 20, 21); отозвать согласие на обработку ПД; возразить против решения, основанного исключительно на автоматизированной обработке (ст. 16 Закона № 152-ФЗ); обжаловать действия (бездействие) Оператора в Роскомнадзор или в суд; на защиту своих прав и законных интересов, включая возмещение убытков и компенсацию морального вреда; удалить загруженные материалы («Пройти заново» / «Сбросить и переснять») и потребовать удаления своих ПД.

9.2. Обращение направляется через форму обратной связи в приложении (Личный кабинет) или по адресу электронной почты Оператора **help@gramaton.pro**. Обращение содержит: фамилию, имя, отчество (при наличии), номер телефона, привязанный к Учётной записи, и суть обращения.

9.3. Оператор рассматривает обращение и направляет ответ в срок, установленный ч. 1 ст. 20 Закона № 152-ФЗ (10 (десять) рабочих дней со дня получения обращения; срок может быть продлён не более чем на 5 (пять) рабочих дней с направлением мотивированного уведомления), если законом не установлен иной срок. При отзыве согласия обработка прекращается, а ПД уничтожаются в срок, не превышающий 30 (тридцати) дней (ч. 5 ст. 21 Закона № 152-ФЗ), за исключением данных, подлежащих хранению в силу закона.

9.4. Порядок рассмотрения обращений, связанных с отказом в допуске (ограничением допуска), определяется разделом А5 настоящего Приложения (в том числе сроки по п. 5.2 и отмена меры по п. 5.3).

В10. Специфика Сервиса

Биометрические персональные данные. Не обрабатываются (решение Оператора от 29.09.2026). Изображение лица (селфи) не запрашивается, не собирается и не хранится; автоматическое распознавание лиц и формирование биометрического шаблона не применяются; сличение изображения лица с фотографией в документе автоматизированными средствами не производится; биометрическая идентификация и аутентификация не осуществляются; подключение библиотек и сервисов распознавания лиц не допускается. Ранее загруженные изображения лица (в тестовых заявках) удалены; тестовое изображение в хранилище документов удалено 29.09.2026. Вместе с тем в справочниках и настройках панели проверки сохраняются **устаревшие технические коды**, относящиеся к селфи (типы документов «селфи», «селфи с документом»; причина решения «селфи не совпадает с документом»), а документ «Перечень ИСПДн и классификация» содержит биометрические ПД в составе обрабатываемых данных ИСПДн-1. Если в будущем потребуются биометрическая идентификация, она вводится исключительно через Единую биометрическую систему (ЕБС) в порядке Федерального закона от 29.12.2022 № 572-ФЗ, с отдельным письменным согласием субъекта, предварительным уведомлением Роскомнадзора и отдельной оценкой воздействия на права субъектов.

Специальные категории ПД. Оператор целенаправленно не запрашивает специальные категории. Из предъявленных документов могут следовать сведения о гражданстве и национальной принадлежности (документы иностранного гражданина, миграционные документы), а также сведения о состоянии здоровья — в объёме, содержащемся в предъявленных документах (отметки, справки, полис ДМС); сведения о судимости — только при добровольном предъявлении соответствующего документа. Такие сведения обрабатываются в объёме, необходимом для целей верификации, и требуют письменного согласия субъекта (ст. 10 ч. 2 п. 1 Закона № 152-ФЗ).

Копии документов как чувствительные данные. Загружаемые изображения документов содержат сведения, отнесённые к обычным и (или) специальным категориям ПД, и обрабатываются с повышенными мерами защиты (B8): хранение в защищённом каталоге и (в контуре панели) в зашифрованном виде, выдача только по подписанной ссылке с коротким сроком действия, маскирование в интерфейсе проверяющего, обязательная причина раскрытия, полный аудит доступа. Экспорт материалов заявки («экспорт доказательств») доступен только отдельным ролям и фиксируется в журнале аудита.

Результат распознавания и его пределы. Распознавание выполняется средствами, работающими на инфраструктуре Оператора, без передачи изображений внешним сервисам. Результат носит предварительный характер, точность не гарантируется, результат **не является** установлением личности, сличением изображения лица или биометрической обработкой. Пользователь вправе подтвердить или исправить извлечённые значения. При этом распознанный текст документа сохраняется целиком, что может включать сведения, не являющиеся необходимыми для целей обработки;

Как фактически проверяется подлинность. На дату редакции проверка обеспечивается визуальным контролем уполномоченного лица Оператора по изображениям документов, сопоставлением сведений между документами и с персональной картой, а также автоматическими сигналами риска (нечитаемое изображение, вероятный дубликат, просроченный документ, расхождение данных, признаки изменения файла). Запросы в государственные информационные системы (ЕСИА, ведомственные реестры МВД, ФНС) в контуре верификации **не выполняются**; проверка сведений о статусе плательщика налога на профессиональный доход, предусмотренная п. 12.2.1 Соглашения, и идентификация через ЕСИА (п. 12.2.2 Соглашения, ч. 2 ст. 5 Закона № 289-ФЗ) обеспечиваются иными средствами и контурами Экосистемы; их реализация применительно к Сервису «Верификация» отнесена к открытым позициям.

Принятие решений. Решения по заявкам принимает уполномоченное лицо Оператора с фиксацией решения, причины и исполнителя в журнале решений и в журнале аудита. Сервис предусматривает числовой показатель (скоринг) заявки и настраиваемые правила (порог авто-одобрения, порог для уровня L1, доля контрольной выборки QA); При вводе автоматизированного принятия решений, порождающих юридические последствия, применяются требования ст. 16 Закона № 152-ФЗ (право субъекта возразить против решения, основанного исключительно на автоматизированной обработке, и получить разъяснения).

Несовершеннолетние. Сервис предназначен для лиц, обладающих необходимой дееспособностью; отдельная документальная проверка возраста в Сервисе на дату редакции не проводится. При выявлении признаков использования Сервиса лицом, не обладающим необходимой дееспособностью, допуск ограничивается в порядке п. А3.7.

Иностранные граждане и лица без гражданства. Обрабатываются документы, предусмотренные для соответствующих категорий (патент, вид на жительство, миграционная карта, карта иностранного гражданина, «зелёная карта», миграционный учёт, полис ДМС). Обработка специальных категорий ПД (гражданство, национальная принадлежность) — в объёме, следующем из документов (B2). Требования трудового законодательства к соответствующим видам деятельности обеспечиваются иными приложениями (в частности, Приложением № 1).

Тайна связи и переписки. Сервис не обрабатывает содержание переписки Пользователей; обмен сообщениями обеспечивается Сервисом «Мессенджер» (Приложение № 9). Сведения о фактах передачи сообщений и содержание переписки предметом настоящего Приложения не являются (ст. 23–24 Конституции РФ, ст. 63 Федерального закона «О связи»).

Геолокация. Координаты местоположения в Сервисе не обрабатываются.

Уведомления. Пользователю могут направляться служебные уведомления о статусе заявки. Рекламные и маркетинговые сообщения направляются только при наличии отдельного согласия (ст. 18 Федерального закона «О рекламе»).

Кадровый контур панели. Панель проверки содержит также кадровый контур (учёт работников, кадровое делопроизводство). Обработка ПД работников настоящим Приложением **не регулируется** и осуществляется в соответствии с отдельными документами Оператора; разграничение доступа к контурам обеспечивается ролевой моделью (B8).

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

| Данные | Цель | Основание | Срок | Получатель | |---|---|---|---|---| | Идентификатор Учётной записи (uuid), данные аутентификации | доступ к Сервису, сопоставление заявки с Пользователем | ст. 6 ч. 1 п. 1, 5 | срок использования Учётной записи; при удалении — запись удаляется | сервис аутентификации Экосистемы; уполномоченные лица Оператора (в объёме заявки) | | ФИО, дата и место рождения, пол, гражданство | идентификация заявителя, проверка соответствия данных документам | ст. 6 ч. 1 п. 1; ст. 9; ст. 10 ч. 2 п. 1 (спецкатегории) | 5 лет (одобренные) / 1 год (отклонённые, пересъёмка, эскалация) от даты решения; затем обезличивание | уполномоченные лица Оператора | | Реквизиты документов (вид, серия/номер, дата выдачи, орган выдачи, срок действия) | проверка подлинности и действительности документов | ст. 6 ч. 1 п. 1, п. 5 | то же | уполномоченные лица Оператора | | Реквизиты иных документов (прописка, СНИЛС, ИНН, ДМС, миграционные документы) | проверка комплектности и соответствия документов категории | ст. 6 ч. 1 п. 1; ч. 2 ст. 5 Закона № 289-ФЗ (для Партнёра) | то же | уполномоченные лица Оператора | | Изображения документов (JPEG/PNG/PDF, до двух сторон) | визуальная проверка подлинности документов | ст. 6 ч. 1 п. 1 | 5 лет / 1 год от даты решения (контур панели); обработчики (объектное хранилище, ЦОД в РФ) по поручению | | Распознанный текст (raw_text) и извлечённые поля (extracted) | предварительное заполнение и сверка данных; удобство проверки | ст. 6 ч. 1 п. 1, п. 5 | в составе заявки (до обезличивания) | уполномоченные лица Оператора (в маскированном виде, если нет права на ПД) | | Персональная карта (подтверждённые поля) | ведение данных Пользователя, повторное использование в заявках | ст. 6 ч. 1 п. 1, п. 5 | до удаления Учётной записи Пользователя | уполномоченные лица Оператора; Пользователь | | Статус верификации, признак категории, статус документов | допуск к функциям Сервисов («Подработка», «Такси») | ст. 6 ч. 1 п. 5; ч. 2 ст. 5 Закона № 289-ФЗ | до изменения статуса; запись — в составе заявки | Сервисы «Подработка», «Такси» (только статус) | | Решения, причины решений, сигналы риска | принятие и подтверждение решения, разбор споров, антифрод | ст. 6 ч. 1 п. 1, 2, 5 | 5 лет / 1 год от даты решения; после обезличивания — как метаданные | уполномоченные лица Оператора; госорганы по мотивированному запросу | | Метаданные файлов (sha256, размер, MIME, результат антивирусной проверки, ключ хранилища) | обеспечение целостности и безопасности обработки | ст. 6 ч. 1 п. 2, 5 | в составе заявки; журналы — 3 года | уполномоченные лица Оператора; обработчики по поручению | | Технические данные (IP-адрес, user-agent, данные сессии) | безопасность, предотвращение несанкционированного доступа | ст. 6 ч. 1 п. 2, 5 | 1 год | уполномоченные лица

Оператора (журналы) | | Журнал аудита (входы/выходы, отказы доступа, решения, просмотр и раскрытие ПД, экспорт, обезличивание) | внутренний контроль, безопасность, подтверждение действий | ст. 6 ч. 1 п. 2; ст. 18.1, 19 | 3 года | уполномоченные лица Оператора (роли аудита и контроля); госорганы по закону | | Служебные ПД уполномоченных лиц (учётная запись, роль, хеш пароля, секрет двухфакторной аутентификации) | управление доступом, служебный учёт | ст. 6 ч. 1 п. 2; ст. 18.1, 19 | до отключения учётной записи + срок хранения журналов | администраторы системы (в объёме прав) | | Контактные данные Учётной записи (телефон, e-mail) | служебные уведомления о статусе заявки | ст. 6 ч. 1 п. 5 | срок использования Учётной записи | сервис доставки уведомлений (по поручению); Пользователь | | Обращения, жалобы и материалы их рассмотрения | реализация прав субъекта, разбор споров, обжалование | ст. 6 ч. 1 п. 1, 2 | 3 года | уполномоченные лица Оператора; госорганы по мотивированному запросу | | Факты согласий (документ, версия, дата, IP, user-agent) | подтверждение заключения договора и получения согласий | ст. 6 ч. 1 п. 2, 5 | срок использования Учётной записи + 3 года | по запросу субъекта; госорганы по закону |
