

Mask Gate — поручение на обработку ПДн, субпроцессоры и ответственность

Mask Gate · trust pack · версия 1.1 · дата 25.10.2026 · проект документа, публикация — после подтверждения владельца

Версия: 1.1 · **Дата:** 25.10.2026 · **Статус:** проект документа, публикация — после подтверждения владельца.

Документ: trust pack, файл 3 из 4. Соседние: «Архитектура безопасности», «Обработка ПДн и 152-ФЗ», «Качество детекции».

Что это. Шаблон поручения на обработку персональных данных по ч. 3 ст. 6 152-ФЗ (для B2B-клиентов, которым нужно передать обработку части ПДн) + список субпроцессоров + лимиты ответственности и контакты. **Шаблон не является юридической консультацией:** перед подписанием его проверяет юрист клиента и юрист оператора, реквизиты и приложения заполняются сторонами. Мы не утверждаем, что этот текст «соответствует 152-ФЗ» — мы приводим его как рабочую заготовку, составленную по требованиям нормы.

1. Обязательные элементы поручения по ч. 3 ст. 6 152-ФЗ

Закон требует, чтобы в поручении были определены (цитата по тексту нормы):

1. **перечень персональных данных**, обработка которых поручается;
2. **перечень действий (операций)** с ПДн, которые будет совершать обработчик;
3. **цели обработки**;
4. **обязанность соблюдать конфиденциальность** ПДн;
5. **требования ч. 5 ст. 18 и ст. 18.1 152-ФЗ** (документы/локальные акты оператора и меры по обеспечению обязанностей);

1. **обязанность по запросу оператора** в течение срока действия поручения, в том числе до обработки, предоставлять документы и иную информацию, подтверждающие принятие мер и соблюдение требований;

1. **обязанность обеспечивать безопасность** ПДн при обработке, включая требования к защите по ст. 19;
2. **требование уведомлять оператора** о случаях, предусмотренных ч. 3.1 ст. 21 152-ФЗ (инциденты с ПДн).

Также по закону: лицо, обрабатывающее ПДн по поручению, **не обязано получать согласие субъекта** (ч. 4); ответственность перед субъектом за действия обработчика несёт **оператор** (ч. 5); если обработчик — иностранное лицо, ответственность перед субъектом несут и оператор, и обработчик (ч. 6). Источник текста нормы: [ст. 6 152-ФЗ](#).

2. Шаблон поручения (редакция для согласования)

Ниже — рабочая заготовка. Поля в квадратных скобках заполняются сторонами. Все сроки уведомлений, кроме прямо указанных законом, — **договорные** и согласуются сторонами.

Поручение на обработку персональных данных № [номер] от [дата]

Оператор: [полное наименование/ФИО, ИНН, ОГРН/ОГРНИП, адрес], в лице [должность, ФИО], действующего на основании [документ] (далее — «Оператор»).

Обработчик: Индивидуальный предприниматель Цымбалюк Андрей Вадимович, ИНН 503123539105, запись в реестре операторов персональных данных № 77-25-184814 (далее – «Обработчик»).

1. Предмет

- 1.1. Оператор поручает, а Обработчик принимает на себя обработку персональных данных, указанных в Приложении 1 к настоящему поручению, в объёме и целях, указанных в разделах 2 и 3.
- 1.2. Обработка осуществляется в рамках договора [реквизиты основного договора/оферты] (далее – «Договор») и исключительно в целях исполнения Договора.

2. Перечень персональных данных и действий

2.1. **Перечень ПДн** (заполняется Оператором; допускается ссылка на категории, передаваемые на проверку): [например: ФИО; паспортные данные; СНИЛС; ИНН; номер банковской карты; номер телефона; адрес электронной почты; адрес регистрации; иные категории, перечисленные в Приложении 1].

2.2. **Действия (операции) с ПДн**, совершаемые Обработчиком:

- получение ПДн от Оператора по API/через интерфейс сервиса;
- анализ (детекция) и маскирование/удаление/блокировка ПДн в соответствии с политикой сервиса;
- при включённом Оператором обратном режиме – хранение зашифрованных пар «токен–значение» в течение

установленного срока (по умолчанию 30 суток) и их возврат по запросу Оператора;

- ведение журнала аудита **без содержимого** (категории находок, HMAC-метки значений, время, origin);
- удаление ПДн по истечении сроков и по запросу Оператора;
- предоставление Оператору отчётов о находках и статистики.

2.3. Обработчик **не вправе**: передавать ПДн третьим лицам, кроме субпроцессоров, перечисленных в разделе 5 (и только в объёме, необходимом для оказания услуг); использовать ПДн в собственных целях; осуществлять трансграничную передачу ПДн без письменного указания Оператора.

2.4. При использовании интеграции с внешней LLM (ВУОК) по указанию Оператора Обработчик передаёт внешнему провайдеру **только прошедший маскирование текст**; выбор провайдера, его условия и ответственность за трансграничную передачу (ст. 12 152-ФЗ) несёт Оператор. Если такая интеграция не используется, внешняя передача не выполняется.

3. Цели обработки

3.1. Проверка текстов и документов на наличие ПДн; маскирование/удаление/блокировка ПДн; формирование отчёта о находках; ведение аудита и статистики; поддержка Оператора; исполнение Договора.

4. Конфиденциальность и безопасность

4.1. Обработчик обязуется соблюдать конфиденциальность ПДн (ст. 7 152-ФЗ) и не раскрывать их третьим лицам, кроме случаев, предусмотренных законом и разделом 5.

4.2. Меры безопасности (в терминах ст. 18.1 и ст. 19 152-ФЗ):

Требование	Реализация
минимизация	тексты обрабатываются в памяти, не накапливаются; файлы не сохраняются после разбора

Требование	Реализация
шифрование при хранении	vault: AES-256-GCM, ключ хранится отдельно от БД (<code>core/vault.py</code>)
шифрование при передаче	TLS 1.2/1.3 (<code>nginx/default.conf</code>)
целостность журнала	HMAC-SHA256-цепочка, межфайловые якоря (<code>core/audit.py</code>)
разграничение доступа	роли, JWT, API-ключи только в виде хешей
сроки хранения	vault — 30 суток; аудит — 180 суток; логи — ≥ 30 суток; бэкапы — 30 суток
удаление	удаление аккаунта/данных, janitor, окно резервных копий 30 суток

4.3. Обработчик предоставляет Оператору по его запросу документы и информацию, подтверждающие принятие мер, в течение [5] рабочих дней с даты запроса.

4.4. Обработчик уведомляет Оператора об инциденте с ПДн **незамедлительно, но не позднее 24 часов** с момента обнаружения (договорный срок; законный срок уведомления РКН для оператора — 24 часа, ч. 3.1 ст. 21 152-ФЗ, — остаётся на Операторе). Уведомление содержит: время, обстоятельства, затронутые категории данных, принятые меры.

5. Субпроцессоры

5.1. Обработчик вправе привлекать субпроцессоров **только из перечня** (раздел 6). Изменение перечня — с уведомлением Оператора не менее чем за [30] дней; Оператор вправе возразить.

5.2. Обработчик остаётся ответственным перед Оператором за действия субпроцессоров.

6. Срок, возврат и уничтожение

6.1. Поручение действует в течение срока Договора и [срок хранения по закону] после его прекращения.

6.2. По прекращении поручения Обработчик прекращает обработку, уничтожает ПДн (включая vault и резервные копии в окне 30 суток) и подтверждает уничтожение актом/уведомлением, кроме данных, которые обязан хранить по закону (например, платёжные записи).

7. Ответственность

7.1. Ответственность сторон — по Договору и оферте. Ответственность перед субъектом за действия Обработчика несёт Оператор (ч. 5 ст. 6 152-ФЗ); Обработчик отвечает перед Оператором.

7.2. Совокупная ответственность Обработчика ограничена суммой последнего платежа по Договору (как в разделе 8 действующей оферты сервиса). Для B2B-договора стороны вправе согласовать иной лимит.

8. Прочее

8.1. Во всём, что не урегулировано поручением, стороны руководствуются Договором и законодательством РФ.

8.2. Поручение составлено в двух экземплярах, имеющих равную юридическую силу.

Подписи сторон: [Оператор] / [Обработчик].

3. Субпроцессоры (инфраструктура SaaS)

Субпроцессор	Роль	Какие данные затрагивает	Подтверждение
Beget (Санкт-Петербург)	хостинг виртуального сервера	все данные SaaS-инсталляции (БД, vault, аудит, логи, бэкапы)	утверждение оператора об инфраструктуре; код его не подтверждает — заявлено на страницах /security и /
ЮKassa	приём платежей	платёжные данные; реквизиты карт обрабатываются провайдером, в сервисе не хранятся	код core/payments_yookassa.py, переменные YOOKASSA_* (.env.example); храним только сумму/статус/идентификатор
Провайдер LLM — сценарий «чат» (DeepSeek, api.deepseek.com)	генерация ответа в чате	только прошедший маскирование текст; ключ — наш MG_CHAT_LLM_KEY, адрес — фиксированный allowlist	код core/llm_client.py, api/chat_routes.py; бэкенд реализован, публичный запуск — по решению владельца; передача возможна только при заданном ключе
Провайдер SMTP (транзакционная почта)	доставка кодов входа и писем	email пользователя, код входа (в БД — только хеш)	код core/mailer.py; конкретный провайдер задаётся SMTP_HOST и в репозитории не зафиксирован — уточняется у оператора
Яндекс.Метрика	веб-аналитика	IP, cookie, поведение на сайте — только после согласия на cookie-баннер	ui/js/metrika.js, MG_METRIKA_ID; Webvisor отключён; на on-prem выключено
GitHub / GHCR	хранение кода и образов	клиентские данные не обрабатываются	процесс сборки/поставки; не является обработчиком ПДн

Self-hosted: субпроцессоры SaaS к обработке не привлекаются — всё работает в контуре клиента, поставка и лицензия не передают данные вендору (лицензия — офлайн-токен Ed25519).

4. Лимиты ответственности и контакты

- **Лимит ответственности:** совокупная ответственность Исполнителя ограничена суммой последнего платежа Пользователя (раздел 8 оферты; для B2B-договора может быть согласован иной лимит).
- **Сервис «как есть»:** Исполнитель не гарантирует отсутствие ошибок и не несёт ответственности за убытки, кроме случаев, предусмотренных законом (раздел 8 оферты).
- **Сертификатов, аудитов, SLA нет** — см. документ 1; обещаний, которых нет, в этом пакете нет.
- **Контакты:**
 - безопасность, инциденты, уязвимости: security@maskgate.ru;
 - общие вопросы и договоры: контакты Исполнителя в разделе 10 оферты (/offer);
 - оператор ПДн: ИП Цымбалюк Андрей Вадимович, ИНН 503123539105, запись в реестре операторов № 77-25-184814.

5. Что в этом шаблоне помечено как «нет/не подтверждено»

- юридическая сила шаблона: **не проверен юристом на стороне сервиса** — это заготовка для согласования;
- фактическое имя SMTP-провайдера SaaS: **не зафиксировано в репозитории** — уточняется у оператора;

- размещение на Beget: **утверждение оператора**, кода/договора в репозитории нет;
- страховка ответственности (страхование киберрисков): **нет данных**;
- программа bug bounty: **отсутствует** (есть канал security@maskgate.ru).

Документ не является юридическим заключением. Сертификатов, независимого аудита и SLA у сервиса нет — это прямо указано в тексте.
Вопросы: security@maskgate.ru