

Условия обработки данных компании

Редакция от 2 октября 2026 года

Документ определяет конфиденциальность бизнес-данных и общие условия поручения обработки персональных данных при использовании AveCor. Он предназначен для заказчика, от имени которого в законном порядке действует уполномоченный представитель.

Условия применяются к данным согласованных подключений. Для каждого подключения заказчик и AveCor определяют состав и цель обработки, доступные функции и порядок выгрузки. Настоящий документ не разрешает передачу любых сведений компании вне согласованного поручения.

Ключевые условия для заказчика

- **Хранение:** рабочие данные размещаются в России; география конкретного подключения определяется до передачи данных. Внешние зашифрованные резервные копии размещаются в хранилище региона Санкт-Петербург. Подробности в разделе 6.
- **Защита:** защищённая передача, проверка полномочий, разграничение доступа компаний и шифрование внешних резервных копий. Чужие пользователи не получают права читать или выгружать данные вашей компании. Подробности в разделе 5.
- **После окончания оплаты:** обновление данных останавливается; рабочие данные бесплатно сохраняются 90 календарных дней для выгрузки и возобновления доступа.
- **Удаление:** предупреждение направляется не позднее чем за 7 дней. Если доступ не продлён, рабочие данные удаляются без дополнительного согласования, затем направляется подтверждение. Более ранние законные требования об удалении имеют приоритет. Подробности в разделе 8.

1. Стороны и распределение ролей

Индивидуальный предприниматель Пенкин Александр Николаевич

ИНН 230802241140

ОГРНИП 326237500008453

Почтовый адрес для корреспонденции и претензий: 350040, Краснодарский край, г. Краснодар, а/я 15.

Электронная почта: info@avecor.ru.

Телефон поддержки: [8 800 550 50 40](tel:88005505040).

- 1.1. Заказчик определяет цели обработки данных своей деятельности и несёт обязанности оператора в отношении персональных данных своих работников, покупателей, партнёров и иных людей, когда закон относит эти данные к его обработке.
- 1.2. AveCor обрабатывает переданные персональные данные по поручению заказчика только в пределах согласованных целей и операций. В отношении собственных учётных записей, поддержки, безопасности и обязательных документов AveCor может выступать самостоятельным оператором согласно [политике конфиденциальности](#).
- 1.3. Неперсональные сведения о бизнесе охраняются как конфиденциальные на условиях этого документа. Режим коммерческой тайны не возникает только из загрузки: заказчик самостоятельно выполняет предусмотренные законом требования к установлению такого режима, если он ему нужен.

2. Конкретизация поручения до подключения

- 2.1. Для каждого источника стороны до передачи данных согласуют описание подключения в заказе, договоре или воспроизводимой электронной форме. В нём определяются: заказчик и пространство; источник; цель; категории субъектов; перечень полей и файлов; операции; срок; необходимые получатели и подрядчики; место хранения и допустимая география передачи; порядок выгрузки, удаления и взаимодействия по обращениям.
- 2.1.1. Описание подключения подтверждает лицо, уполномоченное действовать от имени заказчика. Согласование сохраняется вместе с содержанием поручения, применённой редакцией, датой и сведениями о подтвердившем лице. Назначение роли в интерфейсе не заменяет необходимых полномочий. Передача начинается только в пределах подтверждённого поручения.
- 2.2. Допустимые цели в пределах выбранной функции: объединение показателей выбранных бизнес-систем, построение отчётов и воронки, анализ эффективности рекламы и продаж, техническое сопровождение выбранного подключения. Иные цели требуют отдельного основания и согласования.
- 2.3. Возможные категории людей: работники и уполномоченные представители заказчика, покупатели, потенциальные клиенты, контактные лица контрагентов. В поручение включаются только категории, необходимые конкретному источнику; наличие этого списка в общем документе не разрешает все категории сразу.
- 2.4. Возможные данные: имя, деловые контакты, идентификатор клиента, сведения о взаимодействии, заказе, оплате и договоре, нужные для согласованной аналитики. Файлы, записи и расшифровки звонков включаются только при отдельно выбранной функции и законном основании. Перечень конкретных полей ограничивается согласованным подключением.

2.5. Специальные категории персональных данных, биометрия для установления личности, государственная тайна, полные платёжные реквизиты карты, пароли пользователей источника и иные избыточные сведения исключаются из обычного поручения. Для отдельных законных сценариев требуется самостоятельное согласование и необходимые меры защиты.

3. Законность исходных данных

3.1. Заказчик подтверждает право получить, использовать и передать сведения для согласованной цели, включая право поручить обработку другому лицу. Где закон требует согласия субъекта на поручение или передачу, заказчик обеспечивает его до передачи.

3.2. Заказчик предоставляет людям необходимые сведения об обработке, выполняет требования к трудовым данным и правила записи разговоров. Согласие представителя заказчика или подателя заявки не заменяет согласия каждого человека там, где оно требуется.

3.3. По обоснованному запросу заказчик подтверждает необходимое основание в соразмерном объёме. AveCor вправе приостановить конкретную неправомерную передачу; такое право не освобождает AveCor от собственных обязанностей и не означает презумпции нарушения заказчика.

3.4. Данные источника получаются через разрешённый интерфейс и законно предоставленный доступ. Стороны не обходят ограничения источника и не используют чужие полномочия. Если поставщик источника действует как самостоятельный оператор, его обязанности определяются отдельно.

4. Операции и пределы использования

4.1. В согласованном поручении могут быть разрешены получение, запись, систематизация, накопление, хранение, уточнение по указанию, извлечение, сопоставление, расчёт показателей, предоставление результата уполномоченным пользователям заказчика, ограниченная передача согласованному подрядчику, блокирование, удаление и уничтожение. Не включённые операции не разрешаются автоматически.

4.2. AveCor не продаёт сведения заказчика, не публикует их, не использует для чужой рекламы и не объединяет идентифицируемые данные разных заказчиков для собственных несогласованных целей.

4.3. Материалы заказчика не используются для обучения общей модели искусственного интеллекта на основании одного подключения аналитики. Такое использование, если вообще будет предложено, требует отдельного добровольного основания и не должно быть условием обычного доступа.

4.4. Технические секреты интеграции используются только для выбранного подключения и передаются защищённым способом. После отзыва подключения AveCor прекращает их использование и удаляет сохранённый секрет; аннулирование токена у поставщика выполняется через его интерфейс в согласованном с заказчиком порядке. Пароль человека от источника не должен запрашиваться в обычной переписке.

5. Конфиденциальность и безопасность

5.1. Конфиденциальными являются переданные бизнес-данные, содержание документов, настройки интеграций, технические секреты и результаты анализа, которые законно не стали общедоступными. Права на исходные материалы сохраняются у их обладателей.

5.2. AveCor обеспечивает доступ только для уполномоченных лиц по необходимости, обязательства конфиденциальности и меры безопасности по требованиям статей 18.1 и 19 Закона № 152-ФЗ и применимым подзаконным актам. При чтении, изменении и выгрузке рабочих данных сервер проверяет пользователя, действующее членство в компании и необходимые полномочия. Одного идентификатора компании или ссылки на файл недостаточно для доступа. Пользователи других компаний и исключённые участники не получают доступ к рабочим данным заказчика.

5.3. Заказчик управляет списком своих участников и их ролями, исключает ненужный доступ, защищает собственные устройства и законно предоставляет доступы источников. Каждая сторона отвечает за свою область защиты.

5.4. По обоснованному запросу AveCor до начала и в ходе поручения предоставляет сведения и документы, подтверждающие выполнение относящихся к поручению требований закона и мер защиты, с учётом конфиденциальности других заказчиков и защиты секретов.

5.5. Раскрытие по обязательному законному требованию ограничивается нужным объёмом. Заказчик уведомляется, когда это разрешено законом. Публичное использование его названия, логотипа или результатов в кейсе требует отдельного разрешения.

5.6. Обмен данными с AveCor осуществляется через защищённые соединения HTTPS/TLS. Доступ к сведениям компании предоставляется после проверки пользователя, его действующего членства и полномочий. Пароли хранятся в виде криптографических хешей. Внешние резервные копии шифруются до передачи в хранилище. Доступ к средствам восстановления и техническим секретам ограничивается уполномоченными лицами; они не публикуются и не передаются в обычной переписке.

5.7. Чтение, скачивание и выгрузка разрешаются только владельцу и иным уполномоченным участникам в пределах их ролей и доступных функций. Рабочие файлы не выдаются по постоянной общедоступной ссылке. Если используется временная ссылка выгрузки, её действие ограничивается сроком и проверкой предусмотренных полномочий. Уведомление о выгрузке не содержит сами рабочие данные, пароли или токены.

5.8. Защита включает ограничение административного и сетевого доступа, обновление компонентов с учётом выявленных уязвимостей, защиту входа и сеансов, ограничение злоупотреблений, учёт необходимых действий доступа и выгрузки, резервное копирование и реагирование на инциденты. Сведения о защите предоставляются в объёме, который не раскрывает ключи, секреты или данные других заказчиков.

5.9. Меры защиты направлены на предотвращение несанкционированного доступа, копирования, выгрузки, изменения и утраты данных. Выгрузка предоставляется уполномоченному представителю заказчика в согласованном объёме и защищённым способом.

6. Подрядчики, хранение и география

6.1. Привлечение лица, которое будет обрабатывать данные по поручению, предварительно согласуется с заказчиком и оформляется законным договором с соответствующими обязательствами. Заказчику сообщаются необходимая идентификация получателя, задача, данные и география. Название категории «облачный сервис» не заменяет согласование конкретного получателя.

6.2. Рабочие выгрузки, записи звонков и секреты подключений не направляются через обычные почтовые уведомления или мессенджеры. Для поддержки сведения ограничиваются необходимым объёмом и передаются согласованным защищённым способом.

6.3. Перед использованием внешнего сервиса распознавания, искусственного интеллекта или иной обработки согласуются получатель, цели, поля, хранение, география и условия исключения несогласованного использования. Если эти условия невозможно определить законно, передача не начинается.

6.4. Соблюдаются требования локализации и трансграничной передачи. Передача за пределы России не разрешается автоматически этим общим документом. Необходимые уведомления, основания и ограничения определяются до передачи согласно действующему закону.

6.5. AveCor обеспечивает обработку рабочих данных на инфраструктуре в Российской Федерации. Место размещения конкретного подключения и необходимые получатели определяются в согласованном поручении. Внешние зашифрованные резервные копии

размещаются в хранилище региона Санкт-Петербург. Изменение географии или привлечение внешнего сервиса производится с предварительным согласованием по разделу 2 и соблюдением требований закона. Самостоятельные контактные и почтовые процессы описаны отдельно в политике конфиденциальности.

7. Инциденты и обращения субъектов

7.1. При выявлении неправомерной или случайной передачи, предоставления, распространения либо доступа, нарушающих права субъектов, AveCor уведомляет заказчика без неоправданной задержки, но не позднее 12 часов с выявления. Первичное сообщение содержит известные на этот момент обстоятельства; уточнения передаются по мере расследования.

7.2. Сообщение включает характер события, затронутые категории и предварительный объём, возможные последствия, принятые меры и контакт для взаимодействия в известной на этот момент части. Уточнения передаются по мере расследования; первая информация не откладывается до полного выяснения.

7.3. Стороны взаимодействуют для прекращения нарушения, сохранения необходимых доказательств и устранения последствий. Уведомление AveCor заказчику не заменяет уведомления Роскомнадзора оператором в предусмотренные законом сроки, включая 24 часа для первичного и 72 часа для результатов внутреннего расследования в применимых случаях.

7.4. Если человек обращается в AveCor по данным, оператором которых является заказчик, обращение передаётся заказчику без неоправданной задержки. AveCor содействует уточнению, ограничению, выгрузке или удалению по законному указанию и не раскрывает сведения другому человеку без проверки полномочий.

8. Срок, выгрузка и удаление

8.1. Срок активной обработки задаётся конкретным поручением. По окончании оплаченного периода, если следующий период не оплачен, AveCor прекращает получение и обновление данных из источников, включая фоновые задания. При досрочном отказе применяется момент прекращения доступа по пункту 6.1 оферты либо уведомлению о законном прекращении договора Исполнителем. От этой даты начинается период хранения 90 календарных дней. Правило относится к рабочим наборам подключений, файлам и сохранённым отчётам компании; сроки данных тестирования без оплаченного заказа определяются отдельно до передачи таких данных.

8.2. На эти 90 дней сохраняется ограниченное поручение на бесплатное хранение, защиту, выдачу согласованной выгрузки и восстановление работы после продления. Получение новых данных и новая аналитическая обработка в этот период не проводятся.

Заказчик обеспечивает сохраняющееся законное основание хранения включённых персональных данных. Договор с компанией не заменяет необходимого основания обработки сведений её работников или покупателей.

8.3. До удаления владелец или другой уполномоченный представитель может запросить доступные ему исходные данные и сохранённые результаты в согласованном техническом формате. Состав, формат и защищённый способ выгрузки определяются до начала обработки данных по подключению. Если доступ возобновлён до удаления, обновление начинается после восстановления согласованного подключения. Полнота сведений за пропущенный период зависит от возможностей источника и не гарантируется автоматически.

8.4. При прекращении оплаченного доступа AveCor сообщает владельцу компании дату окончания хранения на подтверждённую почту и в кабинете. Не позднее чем за 7 календарных дней до удаления направляет повторное предупреждение с точной датой, объёмом удаляемых рабочих данных и порядком получения выгрузки. Заказчик поддерживает актуальность адреса и доступ своих уполномоченных лиц. Отсутствие ответа, недоставленное письмо или обычный ответ без продления доступа не создают бессрочного хранения.

8.5. Если к окончанию 90 дней оплаченный доступ не продлён, рабочие данные удаляются без отдельного согласия на каждое удаление. AveCor прекращает ограниченное поручение хранения и уничтожает рабочие наборы, файлы и результаты из действующих баз, файловых хранилищ, реплик, кэша и резервных копий. Цикл копий организуется так, чтобы наличие старой копии само по себе не продлевало эти 90 дней и не позволяло вновь восстановить удалённые рабочие данные. После выполненного удаления владельцу направляется подтверждение с датой и объёмом; удалённые сведения не обещаются к восстановлению.

8.6. Законное указание об удалении, утрата основания или иное обязательное требование исполняются раньше окончания 90 дней в предусмотренный законом срок. При прекращении поручения по иному основанию AveCor возвращает или уничтожает данные не позднее 30 дней, если закон или законное указание требуют более короткого срока. Если технически невозможно своевременно уничтожить персональные данные, применяется предусмотренное законом блокирование и последующее уничтожение в установленный предельный срок; это исключительный порядок, а не обычный дополнительный период хранения копий.

8.7. Обязательные договорные, расчётные и иные документы, которые закон требует сохранить, отделяются от рабочих наборов и используются только для оставшейся законной цели в необходимом объёме и на применимый к ним срок. Это исключение не

разрешает сохранять все рабочие выгрузки под видом расчётных документов. Требования о сохранении конкретных доказательств также исполняются в предусмотренных законом пределах.

8.8. Удаление фиксируется; восстановление инфраструктуры не должно вновь активировать ранее уничтоженные данные. По обоснованному запросу предоставляется подтверждение выполнения указания в согласованном объёме. Завершение обработки рабочих данных не означает автоматического удаления всех сведений учётной записи: для них применяются отдельные цели и сроки политики конфиденциальности.

9. Изменения, ответственность и связь

9.1. Новая цель, новый существенный набор данных, получатель или география согласуются до изменения обработки. Необходимое согласие субъекта обеспечивает та сторона, на которую закон возлагает эту обязанность.

9.2. Заказчик отвечает перед субъектами за собственную организацию обработки. AveCor отвечает перед заказчиком за выполнение поручения и собственные нарушения; для коммерческого заказчика применяются допустимые законом пределы договорной ответственности из оферты или индивидуального договора. Это не переносит на заказчика ответственность за действия AveCor и не отменяет обязанности сторон перед законом.

9.3. Заказчик и его уполномоченный представитель направляют указания и вопросы по указанной выше почте. Существенное указание подтверждается воспроизводимым способом с проверкой полномочий. Споры регулируются российским правом и законными правилами подсудности.

10. Паспорт подключения

До передачи данных стороны заполняют и подтверждают паспорт подключения со следующими полями:

- Заказчик, необходимые реквизиты, рабочее пространство и уполномоченный представитель.
- Источник, выбранная функция и конкретная цель обработки.
- Категории людей, перечень полей, файлов и разрешённых операций.
- Начало и срок обработки, основания передачи заказчиком.
- Конкретные получатели и обработчики, их задачи и передаваемые сведения.
- Место хранения, допустимая география и необходимые меры защиты.
- Состав, формат и защищённый способ выгрузки.
- Порядок прекращения, удаления и взаимодействия по запросам и инцидентам.

- Редакции условий, дата и воспроизводимое подтверждение сторон.

Паспорт может оформляться приложением к договору или согласованным электронным документом. Общий перечень возможных сведений в этих условиях не заменяет заполненный паспорт и не разрешает несогласованную передачу.

Связанные документы: [пользовательское соглашение](#), [оферта на платный доступ](#), [политика конфиденциальности](#).