

ДОГОВОР ПОРУЧЕНИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ № _____

г. _____

«__» _____ 20__ г.

Консультант — юридическое лицо или индивидуальный предприниматель, имеющий действующую лицензию на осуществление медицинской деятельности, заключивший с **Исполнителем** настоящий Договор путём акцепта публичной оферты, именуемый в дальнейшем «**Оператор**», с одной стороны, и

Тимербулатов Фанис Тагирович (ИНН 027816879176, статус: самозанятый, адрес регистрации: 628007, г.Ханты-Мансийск, ул.Чехова, д.14, 208), именуемый в дальнейшем «**Исполнитель**», с другой стороны, совместно именуемые «Стороны», заключили настоящий Договор о нижеследующем.

1. Предмет Договора

1.1. Оператор поручает, а Исполнитель принимает на себя обязательство осуществлять обработку персональных данных (далее — ПДн) пациентов/клиентов Оператора в объёме и в целях, указанных в настоящем Договоре, с использованием программно-аппаратного комплекса — информационной системы «**CRM Контактор**», расположенной по адресу: <https://m1mkontakt.ru> (далее — Система).

1.2. Обработка ПДн включает следующие действия:

- сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение);
- извлечение, использование, передачу (Оператору), блокирование, удаление, уничтожение;
- предоставление доступа к ПДн сотрудникам Оператора (консультантам) с соблюдением разграничения прав доступа.

1.3. Цели обработки ПДн:

- документационное обеспечение медицинской деятельности Оператора (в рамках действующей лицензии);
- консультирование пациентов по применению продукции Coral Club и подбор индивидуальных программ оздоровления;
- ведение электронных анкет, историй обращений, результатов опросов;
- коммуникация с пациентом (информирование, обратная связь).

1.4. Обработка специальных категорий ПДн (состояние здоровья, диагнозы, медицинские показатели) осуществляется на законном основании — в связи с осуществлением Оператором медицинской деятельности, подтверждённой лицензией (копия прилагается к настоящему Договору).

2. Перечень обрабатываемых ПДн

2.1. Исполнитель обрабатывает следующие категории ПДн:

- **ФИО** пациента;
- **контактные данные**: номер телефона, адрес электронной почты (опционально);

- **дата рождения;**
- **данные о состоянии здоровья:** жалобы, анамнез, симптомы, результаты опросов, диагностические данные (предоставляются пациентом);
- **данные о назначениях:** рекомендуемые БАДы, программы оздоровления;
- **данные об обратной связи:** отзывы о результатах применения продуктов (при этом отзывы публикуются в обезличенном виде — «Пациент №1, №2...»).

2.2. Обработка ПДн, указанных в п. 2.1, производится исключительно в пределах, необходимых для достижения целей, указанных в п. 1.3.

3. Права и обязанности Исполнителя (техническая и организационная защита)

3.1. Исполнитель обязуется обеспечить защиту ПДн в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 01.11.2012 № 1119 (уровень защищённости — не ниже УЗ-3);
- Приказа ФСТЭК России от 18.02.2013 № 21 (состав организационных и технических мер);
- иных нормативных правовых актов в области защиты ПДн.

3.2. Исполнитель реализует следующие **технические меры защиты информации** (подробное описание приведено в **Приложении № 1** к настоящему Договору, являющемуся его неотъемлемой частью):

Категория мер	Реализация в Системе
Идентификация и аутентификация	Уникальный логин/пароль (bcrypt), двухфакторная аутентификация (PIN-код 4 цифры в мобильном приложении), защита от брутфорса (5 попыток в минуту), токен-аутентификация API (Laravel Sanctum)
Разграничение доступа	Ролевая модель (6 полей: customer, partner, mentor, team_leader, director, admin), иерархический доступ (консультант видит только свои контакты и контакты подчинённых), изоляция анкет по ссылкам
Защита каналов связи	HTTPS/SSL (шифрование всех соединений), CORS-настройки, обязательный Bearer-токен для API-запросов
Защита хранимых данных	Хеширование паролей (bcrypt), отсутствие хранения открытых паролей, обезличивание отзывов о здоровье
Регистрация событий (аудит)	Журнал аудита (таблица audit_logs): логируются входы, CRUD-операции с контактами, создание анкет, отправка доступа, сброс пароля. Автоочистка логов старше 180 дней
Антивирусная защита	Валидация загружаемых файлов (тип, размер до 2MB), ограничение типов (изображения, документы), изоляция хранилища
Защита от утечек	Запрет прямого доступа к файлам (.htaccess), проверка иерархии при скачивании (canViewUserData()), очистка временных файлов
Защита мобильного приложения	Локальный PIN-код (4 цифры) при входе, очистка токена при 401, блокировка после 3 неверных PIN-попыток

3.3. Исполнитель обязуется:

- **Немедленно (в течение 24 часов)** уведомить Оператора о любом факте:
 - несанкционированного доступа к Системе;
 - утечки ПДн;

- сбой в работе системы, повлёкшего утрату или повреждение ПДн;
- получения требования от государственных органов (Роскомнадзор, ФСТЭК, ФСБ) о предоставлении информации или блокировке доступа.
- **Ежеквартально** (по запросу Оператора) предоставлять отчёт о состоянии защищённости Системы (отсутствие критических уязвимостей, результаты внутреннего аудита).
- **Не передавать ПДн третьим лицам** без письменного согласия Оператора, за исключением случаев, предусмотренных законодательством РФ.
- **Обеспечить возможность удаления ПДн** по первому требованию Оператора или при расторжении Договора (срок — не более 10 рабочих дней).

3.4. Исполнитель **не вправе**:

- использовать ПДн в каких-либо иных целях, кроме указанных в п. 1.3;
- копировать ПДн на собственные носители (вне системы);
- передавать доступ к Системе лицам, не уполномоченным Оператором.

4. Права и обязанности Оператора (Консультанта)

4.1. Оператор обязуется:

- Предоставить Исполнителю копию **лицензии на осуществление медицинской деятельности** (при заключении Договора) и уведомлять об изменении статуса лицензии.
- Обеспечить наличие **письменных согласий** пациентов на обработку их ПДн, включая передачу ПДн Исполнителю (в случаях, когда это требуется по закону).
- Не требовать от Исполнителя обработки ПДн, выходящей за пределы целей, указанных в п. 1.3.
- Своевременно уведомлять Исполнителя об отзыве согласия пациентом или об изменении целей обработки.
- Обеспечить, чтобы все сотрудники Оператора, имеющие доступ к Системе:
 - были ознакомлены с настоящим Договором и Политикой обработки ПДн;
 - использовали двухфакторную аутентификацию (PIN-код в мобильном приложении);
 - не передавали свои учётные данные третьим лицам.
- Нести полную ответственность за законность получения и объём ПДн, передаваемых для обработки в Систему.

4.2. Оператор вправе:

- Требовать от Исполнителя подтверждения выполнения мер защиты ПДн.
- Запрашивать журналы аудита за определённый период.
- Блокировать доступ к Системе отдельным сотрудникам в случае нарушения ими условий настоящего Договора.

5. Ответственность Сторон

5.1. **Исполнитель** несёт ответственность перед Оператором за:

- нарушение конфиденциальности ПДн, произошедшее по вине Исполнителя (взлом Системы, утечка через каналы администрирования);
- несвоевременное уведомление об инцидентах (п. 3.3);
- неисполнение обязанности по удалению ПДн при расторжении Договора.

5.2. **Оператор** несёт ответственность перед субъектами ПДн (пациентами) и государственными органами за:

- законность сбора и обработки ПДн (включая действия Исполнителя, если они не выходили за пределы поручения);
- наличие согласий пациентов;
- соблюдение медицинского законодательства при назначении программ оздоровления.

5.3. В случае наложения на Исполнителя **административного штрафа** по ст. 13.11 КоАП РФ (нарушение порядка обработки ПДн), причиной которого явилось неисполнение Исполнителем обязанностей по защите ПДн (установленное вступившим в силу решением суда или постановлением РКН/ФСТЭК), Исполнитель обязуется возместить Оператору сумму уплаченного штрафа в течение 30 календарных дней.

5.4. В случае наложения на Оператора **административного штрафа** или привлечения к гражданско-правовой ответственности перед пациентами по причине действий Исполнителя, выходящих за пределы поручения (например, передача ПДн третьим лицам без согласия Оператора), Исполнитель возмещает Оператору **прямой действительный ущерб** в полном объёме.

5.5. **Ограничение ответственности Исполнителя:** Общая сумма ответственности Исполнителя по настоящему Договору не может превышать сумму, полученную Исполнителем от Оператора за 12 месяцев, предшествующих нарушению, если иное не будет установлено вступившим в силу решением суда при наличии умысла или грубой неосторожности со стороны Исполнителя.

6. Срок действия и порядок расторжения

6.1. Настоящий Договор вступает в силу с момента его акцепта Оператором (подписание в двух экземплярах или электронная подпись) и действует бессрочно до момента расторжения.

6.2. **Расторжение по инициативе Оператора:** Оператор вправе расторгнуть Договор в одностороннем порядке, уведомив Исполнителя за 10 рабочих дней.

6.3. **Расторжение по инициативе Исполнителя:** Исполнитель вправе расторгнуть Договор, уведомив Оператора за 30 календарных дней.

6.4. **Досрочное расторжение** допускается в случаях:

- лишения Оператора лицензии на медицинскую деятельность;
- вступления в законную силу решения суда о запрете обработки ПДн;
- неустранения Исполнителем критических уязвимостей в Системе (уровень CVSS $\geq$ 7,0) в течение 30 дней после письменного уведомления.

6.5. При расторжении Договора Стороны подписывают **Акт о прекращении обработки ПДн**, в котором фиксируется:

- факт удаления или передачи Исполнителем всех ПДн Оператору;
- отсутствие у Исполнителя копий ПДн на любых носителях.

7. Заключительные положения

7.1. Настоящий Договор составлен в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

7.2. Все изменения и дополнения к Договору действительны лишь в том случае, если они совершены в письменной форме и подписаны обеими Сторонами.

7.3. Во всём остальном, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.

7.4. **Приложение № 1** («Технические меры защиты информации ИС «CRM Контактор»») является неотъемлемой частью настоящего Договора.

8. Реквизиты и подписи

Оператор (Консультант):

Полное наименование:

ИНН: _____

ОГРНИП / ОГРН: _____

Лицензия на медицинскую деятельность:

№ _____ от «_» _____ 20 г. (копия
прилагается)

Юридический адрес:

Телефон: _____

Email для официальной переписки:

Подпись: _____ / (ФИО)
М.П. (при наличии)

Исполнитель:

Тимербулатов Фанис Тагирович

ИНН 027816176879

Статус: самозанятый

Адрес регистрации: 628007, г.Ханты-
Мансийск, ул.Чехова, д.14, 208

Телефон: +79048723574

Email для официальной переписки:

support@mlmkontakt.ru

Подпись: _____ / Тимербулатов Ф.Т.

Дата: «__» _____ 20__ г.

Приложение № 1

Технические меры защиты информации ИС «CRM Контактор» (mlmkontakt.ru)

(Настоящее Приложение является неотъемлемой частью Договора поручения
обработки персональных данных № ____ от «_» _____ 20 г.)

1. Идентификация и аутентификация

Мера	Реализация
Уникальный логин/пароль	Каждый пользователь имеет уникальную учётную запись (email/телефон + bcrypt-хеш пароля)
Двухфакторная аутентификация	PIN-код (4 цифры) в мобильном приложении после успешного ввода логина/пароля
Защита от брутфорса	Rate-limiting: 5 попыток входа в минуту (ThrottleAdminLogin, throttle:5,1)

Блокировка неактивных	Поле <code>is_active</code> — деактивированные пользователи не могут войти
Токен-аутентификация API	Laravel Sanctum (Bearer токены, срок жизни 30 дней + возможность refresh)
Автоматический выход	Очистка сессий старше 3 дней

2. Разграничение доступа

Мера	Реализация
Ролевая модель	6 ролей: <code>customer</code> , <code>partner</code> , <code>mentor</code> , <code>team_leader</code> , <code>director</code> , <code>admin</code>
Иерархический доступ	<code>HierarchyService::getFilteredQuery()</code> — консультант видит только свои контакты и контакты подчинённых
Разделение консультант/клиент	Клиенты не имеют доступа к админ-панели (Filament), редиректятся в ЛК
Middleware проверки роли	<code>RedirectCustomersFromAdmin</code> — клиенты перенаправляются
Изоляция анкет	Каждый консультант видит только анкеты, созданные по его персональной ссылке
Составной уникальный индекс	<code>email + role</code> — предотвращает коллизии между учётными записями консультанта и клиента

3. Защита каналов связи

Мера	Реализация
HTTPS/SSL	Все соединения шифруются (SSL-сертификат, актуальный на момент подписания)
Защита API	Все запросы к API требуют <code>Authorization: Bearer <token></code>
CORS	Настроен <code>HandleCors</code> — разрешены только доверенные источники

4. Защита хранимых данных

Мера	Реализация
Хеширование паролей	<code>bcrypt</code> через <code>Hash::make()</code> (каст <code>hashed</code> в модели User)
Отсутствие открытых паролей	Поле <code>plain_password</code> удалено из БД, хранение открытых паролей не предусмотрено
Обезличивание отзывов	<code>testimonials.testimonial_type = 'health_result'</code> — данные публикуются без привязки к конкретному пользователю
Минимизация данных	Поле <code>email</code> в таблице <code>users</code> — nullable (можно использовать только телефон)

5. Регистрация событий (аудит)

Мера	Реализация
Журнал аудита	Таблица <code>audit_logs</code> + сервис <code>AuditService</code>

Логируемые события	Входы в систему, CRUD-операции с контактами, создание анкет, отправка доступа, сброс пароля
Автоочистка	Аудит-логи старше 180 дней удаляются автоматически (по расписанию)
Логирование ошибок	laravel.log — фиксируются все исключения и ошибки системы

6. Антивирусная защита и целостность

Мера	Реализация
Валидация загружаемых файлов	FileUpload — проверка типа файла, размера (максимум 2 MB)
Ограничение типов	Только изображения (jpeg, png, webp) и документы (pdf, docx)
Изоляция хранилища	Файлы материалов — в storage/app/public/materials/ с проверкой доступа через контроллер

7. Защита от утечек

Мера	Реализация
Запрет прямого доступа	.htaccess в директории storage/materials/ — запрет прямого обращения
Проверка иерархии при скачивании	MaterialController@download — проверяет canViewUserData()
Очистка временных файлов	Livewire temp-файлы очищаются автоматически
Cookie-баннер	Информирование о сборе cookie + модальное окно с Политикой cookie

8. Организационные меры (документальное обеспечение)

Мера	Реализация
Политика обработки ПДн	Опубликована по адресу: https://mlmkontakt.ru/privacy
Согласие на обработку ПДн	Модальное окно с прокруткой до конца текста + обязательный чекбокс в анкетах
Согласие на передачу данных консультантам	Отдельный текст в модальном окне (информирование)
Настоящий Договор поручения	Публичная оферта доступна для скачивания в формате PDF
Обезличенные отзывы о здоровье	Публикуются как «Пациент №1, №2...» без раскрытия личности
Контакты Оператора	Указаны на странице /privacy: ФИО, ИНН, статус самозанятого, email

9. Защита мобильного приложения (для консультантов)

Мера	Реализация
------	------------

Локальный PIN-код	4-значный PIN при входе в приложение, хранится в защищённом DataStore
Очистка токена при 401	Автоматический сброс токена и редирект на экран логина
Проверка токена при старте	MainActivity проверяет валидность токена перед загрузкой данных
Защита от подбора PIN	3 неверные попытки PIN → полный сброс учётных данных приложения

10. Соответствие нормативным правовым актам (статус на дату Договора)

Документ	Статус соответствия
Федеральный закон от 27.07.2006 № 152-ФЗ	☒ Меры реализованы в полном объёме, необходимом для поручения обработки
Постановление Правительства РФ № 1119 (уровни защищённости)	☒ Уровень защищённости — УЗ-3 (для специальных категорий ПДн с неконфиденциальными каналами)
Приказ ФСТЭК России № 21 (состав мер)	☒ Базовые организационные и технические меры реализованы
Уведомление в Роскомнадзор об обработке ПДн	☐ Не отправлено (Оператор обязан направить уведомление, если является оператором ПДн; Исполнитель — нет)
Аттестация информационной системы	☐ Не проводилась (требуется при обработке ПДн 1 и 2 уровня защищённости. При УЗ-3 аттестация не требуется, но рекомендуется внутренний протокол оценки)

11. Резюме по защищённости

Система «CRM Контактор» (mlmkontakt.ru) соответствует **уровню защищённости УЗ-3** (с элементами УЗ-4) в соответствии с Постановлением № 1119. Реализовано **22 технические меры** и **6 организационных мер**. Критические уязвимости, позволяющие осуществить несанкционированный доступ к ПДн, отсутствуют по результатам внутреннего тестирования.

Рекомендации для Оператора:

- Направить уведомление в Роскомнадзор об обработке ПДн (если Оператор ещё этого не сделал).
- Обеспечить наличие письменных согласий пациентов на передачу их ПДн в CRM-систему.

Рекомендации для Исполнителя:

- Провести внутренний протокол оценки соответствия ФСТЭК (акт комиссии).
- При увеличении объёмов обрабатываемых ПДн (более 10 000 субъектов или высокорисковые категории) рассмотреть вопрос о проведении аттестации.

Приложение № 1 составлено Исполнителем и является достоверным отражением состояния защищённости ИС на дату подписания Договора.

Подпись Исполнителя: _____ / Тимербулатов Ф.Т.