УТВЕРЖДАЮ

Индивидуальный предприниматель
Козарезова Маргарита Витальевна

_____ / Козарезова М.В. /

«01» июня 2026 г.

ПОЛОЖЕНИЕ
о защите персональных данных

1. Общие положения

1.1. Настоящее Положение о защите персональных данных, далее — «Положение», определяет порядок защиты персональных данных, обрабатываемых индивидуальным предпринимателем Козарезовой Маргаритой Витальевной, далее — «Оператор», при осуществлении деятельности фитнес-студии «ОСНОВА женского тела» / «Основа».

1.2. Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами Российской Федерации в области персональных данных, а также внутренними документами Оператора.

1.3. Цель настоящего Положения — обеспечить защиту персональных данных клиентов, потенциальных клиентов, посетителей сайта, пользователей онлайн-форм, мессенджеров, социальных сетей, работников, подрядчиков и иных лиц от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

1.4. Настоящее Положение является внутренним локальным документом Оператора и обязательно для исполнения всеми лицами, имеющими доступ к персональным данным.

1.5. Персональные данные являются конфиденциальной информацией. Лица, получившие доступ к персональным данным, обязаны не раскрывать их третьим лицам и не распространять без законного основания.

1.6. Обработка и защита персональных данных осуществляются с соблюдением принципов законности, минимизации объема данных, ограничения доступа, конфиденциальности, актуальности и безопасности.

2. Термины и определения

2.1. Персональные данные — любая информация, относящаяся к прямо или косвенно определенному либо определяемому физическому лицу.

2.2. Оператор — индивидуальный предприниматель Козарезова Маргарита Витальевна, самостоятельно организующая и осуществляющая обработку персональных данных, определяющая цели обработки, состав данных и действия с ними.

2.3. Обработка персональных данных — любое действие или совокупность действий с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, использование, передачу, обезличивание, блокирование, удаление и уничтожение.

2.4. Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.5. Доступ к персональным данным — возможность ознакомления, использования, внесения, изменения, передачи или удаления персональных данных.

2.6. Конфиденциальность персональных данных — обязанность не раскрывать персональные данные третьим лицам без согласия субъекта персональных данных или иного законного основания.

3. Персональные данные, подлежащие защите

3.1. Защите подлежат все персональные данные, обрабатываемые Оператором, включая:

— фамилию, имя, отчество;
— номер телефона;
— адрес электронной почты;
— дату рождения;
— сведения о записи на тренировки;
— сведения об абонементах, посещениях, оплатах, переносах и отменах занятий;
— сведения из анкет, заявок, форм обратной связи;
— сообщения клиентов в мессенджерах, социальных сетях, электронной почте;
— сведения об ограничениях по физической нагрузке, самочувствии и противопоказаниях, которые клиент добровольно сообщает Оператору;
— фото- и видеоматериалы с изображением клиента, если они обрабатываются на основании отдельного согласия;
— технические данные сайта, включая IP-адрес, cookie, сведения о браузере, устройстве, источнике перехода и действиях на сайте;
— данные работников, подрядчиков и представителей контрагентов, если такие данные обрабатываются Оператором.

3.2. Персональные данные могут храниться и обрабатываться:

— на бумажных носителях;
— в CRM-системе;
— в сервисах онлайн-записи;
— в платежных сервисах;
— в электронной почте;
— в мессенджерах;
— в сервисах аналитики сайта;
— в таблицах и файлах внутреннего учета;
— на компьютерах, телефонах и иных устройствах Оператора или уполномоченных лиц;
— в иных информационных системах, используемых для деятельности фитнес-студии.

4. Как Оператор защищает персональные данные

4.1. Оператор применяет правовые, организационные и технические меры защиты персональных данных.

4.2. К правовым мерам защиты относятся:

— утверждение Политики обработки персональных данных;
— утверждение настоящего Положения;
— оформление согласий субъектов персональных данных в необходимых случаях;
— оформление согласий на рекламные рассылки при необходимости;
— оформление согласий на фото- и видеосъемку и публикацию изображения при необходимости;
— заключение договоров и соглашений с подрядчиками, которым передаются персональные данные;
— включение в договоры с подрядчиками условий о конфиденциальности и защите персональных данных;
— назначение лица, ответственного за организацию обработки и защиты персональных данных.

4.3. К организационным мерам защиты относятся:

— ограничение круга лиц, имеющих доступ к персональным данным;
— предоставление доступа только в объеме, необходимом для выполнения рабочих обязанностей;

— ведение перечня лиц, имеющих доступ к персональным данным;
— ознакомление лиц, имеющих доступ к персональным данным, с настоящим Положением;
— запрет передачи персональных данных посторонним лицам без законного основания;
— запрет хранения персональных данных в личных файлах, не предназначенных для работы студии;
— запрет отправки баз клиентов в личные чаты, открытые группы и незащищенные каналы;
— хранение бумажных документов в местах, исключающих доступ посторонних лиц;
— контроль актуальности доступов к CRM, почте, мессенджерам и иным сервисам;
— отзыв доступа у лиц, прекративших работу со студией;
— регулярная проверка соблюдения требований по защите персональных данных.

4.4. К техническим мерам защиты относятся:

— использование паролей для доступа к компьютерам, телефонам, CRM, почте и иным сервисам;
— использование индивидуальных учетных записей там, где это возможно;
— ограничение прав доступа в информационных системах;
— использование антивирусной защиты при необходимости;
— обновление программного обеспечения;
— резервное копирование важных данных при необходимости;
— использование защищенного доступа к сервисам, поддерживающим HTTPS;
— настройка блокировки экрана на рабочих устройствах;
— запрет передачи логинов и паролей третьим лицам;
— хранение паролей способом, исключающим доступ посторонних лиц;
— удаление данных с устройств при прекращении их использования для работы студии.

5. Лица, имеющие доступ к персональным данным

5.1. Доступ к персональным данным предоставляется только лицам, которым он необходим для выполнения рабочих функций.

5.2. Доступ к персональным данным могут иметь:

5.2.1. Индивидуальный предприниматель Козарезова Маргарита Витальевна — полный доступ к персональным данным, необходимым для организации деятельности студии.

5.2.2. Администратор студии — доступ к данным клиентов, необходимым для записи на занятия, связи с клиентами, учета посещений, абонементов, оплат, переносов и отмен.

5.2.3. Тренеры студии — ограниченный доступ к данным клиентов, необходимым для проведения занятий, идентификации клиента, учета посещения и учета добровольно сообщенных ограничений по физической нагрузке.

5.2.4. Маркетолог, SMM-специалист или специалист по рекламе — ограниченный доступ к контактным данным, заявкам, обращениям и материалам, необходимым для коммуникации, рекламы, обработки заявок и публикации материалов при наличии согласия.

5.2.5. Бухгалтер — доступ к данным, необходимым для учета оплат, подготовки документов, налогового и бухгалтерского учета.

5.2.6. IT-специалист, администратор сайта, CRM или технический подрядчик — технический доступ к информационным системам в объеме, необходимом для настройки, сопровождения, устранения ошибок и обеспечения работы сервисов.

5.4. Лица, имеющие доступ к персональным данным, обязаны:

— соблюдать конфиденциальность персональных данных;
— использовать персональные данные только для выполнения рабочих задач;
— не передавать персональные данные третьим лицам без разрешения Оператора;
— не копировать базы клиентов без необходимости;
— не хранить персональные данные на личных устройствах без согласования с Оператором;
— незамедлительно сообщать Оператору о случаях утраты, раскрытия, несанкционированного доступа или иной угрозы безопасности персональных данных.

6. Защита бумажных носителей персональных данных

6.1. Бумажные документы, содержащие персональные данные, хранятся в местах, исключающих свободный доступ посторонних лиц.

6.2. К бумажным документам могут относиться:

— анкеты клиентов;
— согласия на обработку персональных данных;
— согласия на рекламные рассылки;
— согласия на фото- и видеосъемку;
— договоры, заявления, претензии, акты и иные документы.

6.3. Бумажные документы хранятся в папках, шкафах, ящиках или иных местах хранения, доступ к которым имеют только уполномоченные лица.

6.4. Запрещается оставлять документы с персональными данными в открытом доступе: на стойке администратора, в зале тренировок, в зоне ожидания, на ресепшене без присмотра, в местах, доступных клиентам и посетителям.

6.5. При необходимости передачи бумажных документов уполномоченному лицу передача осуществляется способом, исключающим доступ посторонних лиц.

6.6. Бумажные документы, срок хранения которых истек, уничтожаются путем измельчения, сжигания или иным способом, исключающим восстановление содержащихся в них персональных данных.

7. Защита информационных систем

7.1. Информационные системы, в которых хранятся и обрабатываются персональные данные, должны быть защищены от несанкционированного доступа.

7.2. К информационным системам Оператора могут относиться:

— CRM-система;
— сервис онлайн-записи;
— платежный сервис;
— электронная почта;
— мессенджеры;
— сайт и формы обратной связи;
— сервисы аналитики сайта:

— доступ по логину и паролю;
— индивидуальные учетные записи для пользователей, если это поддерживается сервисом;
— ограничение прав доступа в зависимости от роли пользователя;
— использование сложных паролей;
— запрет передачи паролей третьим лицам;
— изменение паролей при риске компрометации;
— отзыв доступа при увольнении, прекращении сотрудничества или изменении функций лица;
— включение двухфакторной аутентификации там, где это возможно и целесообразно;
— использование актуального программного обеспечения;
— ограничение доступа к устройствам, на которых обрабатываются персональные данные;
— блокировка экрана при оставлении устройства без присмотра;
— удаление персональных данных с устройств, которые больше не используются для работы студии;
— резервное копирование важных данных при необходимости.

7.4. Доступ к CRM, сервисам онлайн-записи, почте и иным системам предоставляется только тем лицам, которым такой доступ необходим для выполнения рабочих задач.

7.5. Уровень доступа определяется исходя из принципа минимальной необходимости: пользователь получает только те права, которые нужны ему для выполнения конкретных функций.

7.6. Запрещается использовать общедоступные или небезопасные устройства для входа в CRM, почту и иные системы, содержащие персональные данные, если это может создать риск доступа посторонних лиц.

7.7. Запрещается сохранять пароли в открытых документах, заметках, общих чатах и иных местах, доступных посторонним лицам.

8. Защита данных при работе с подрядчиками и сервисами

8.1. При привлечении подрядчиков и использовании внешних сервисов Оператор принимает меры для обеспечения защиты персональных данных.

8.2. Передача персональных данных подрядчикам допускается только в объеме, необходимом для выполнения соответствующей задачи.

8.3. К подрядчикам и сервисам, которые могут получать доступ к персональным данным, относятся:

— CRM-системы;
— сервисы онлайн-записи;
— платежные сервисы;
— сервисы телефонии, SMS, e-mail и мессенджер-рассылок;
— администраторы сайта;
— хостинг-провайдеры;
— бухгалтеры;
— юристы;
— маркетологи;
— IT-специалисты;
— иные лица и организации, привлекаемые Оператором.

8.4. При заключении договоров с подрядчиками Оператор предусматривает условия о конфиденциальности и защите персональных данных, если подрядчик получает доступ к таким данным.

9. Контроль безопасности персональных данных

9.1. Оператор осуществляет внутренний контроль за соблюдением требований по защите персональных данных.

9.2. Контроль безопасности включает:

— проверку наличия и актуальности согласий на обработку персональных данных;
— проверку доступа сотрудников и подрядчиков к CRM, почте, мессенджерам и иным сервисам;
— проверку соблюдения принципа минимального доступа;
— проверку хранения бумажных документов;
— проверку актуальности паролей и учетных записей;
— проверку удаления доступов у лиц, прекративших работу со студией;
— проверку наличия согласий на рекламные рассылки;
— проверку наличия согласий на фото- и видеосъемку и публикацию изображения;
— проверку соблюдения порядка уничтожения персональных данных;
— анализ инцидентов и принятие мер по их недопущению в будущем.

9.3. Плановая проверка соблюдения требований по защите персональных данных проводится не реже одного раза в год.

9.4. Внеплановая проверка проводится при:

— выявлении нарушения порядка обработки персональных данных;
— утрате документов или устройств, содержащих персональные данные;
— подозрении на несанкционированный доступ;
— изменении CRM, сервиса онлайн-записи, сайта или иных информационных систем;
— поступлении жалобы или обращения субъекта персональных данных;
— изменении законодательства Российской Федерации в области персональных данных.

9.5. По результатам проверки Оператор определяет выявленные нарушения, сроки их устранения и ответственных лиц.

10. Порядок действий при инцидентах

10.1. Инцидентом безопасности персональных данных признается любое событие, которое привело или может привести к неправомерному доступу, уничтожению, изменению, блокированию, копированию, предоставлению, распространению персональных данных или иному нарушению их безопасности.

10.2. К инцидентам относятся:

— утрата бумажных документов;
— утрата телефона, ноутбука или иного устройства с доступом к персональным данным;
— отправка персональных данных не тому адресату;
— публикация персональных данных без согласия;
— взлом учетной записи;
— передача логина или пароля постороннему лицу;
— доступ бывшего сотрудника или подрядчика к CRM, почте или иным сервисам;
— обнаружение персональных данных в открытом доступе;
— иные случаи возможного нарушения безопасности.

10.3. Лицо, выявившее инцидент, обязано незамедлительно сообщить об этом Оператору.

10.4. При выявлении инцидента Оператор:

— фиксирует факт инцидента;
— определяет, какие данные могли быть затронуты;

— ограничивает или блокирует доступ к скомпрометированной системе;
— меняет пароли и отзывает доступы при необходимости;
— принимает меры по прекращению нарушения;
— оценивает необходимость уведомления уполномоченных органов и субъектов персональных данных;
— принимает меры для недопущения повторения инцидента.

10.5. Если инцидент повлек неправомерную передачу, предоставление, распространение или доступ к персональным данным, Оператор действует в соответствии с требованиями законодательства Российской Федерации.

11. Порядок уничтожения персональных данных

11.1. Персональные данные уничтожаются в случаях:

— достижения целей обработки;
— истечения сроков хранения;
— отзыва согласия субъектом персональных данных, если отсутствуют иные законные основания для обработки;
— выявления неправомерной обработки;
— прекращения необходимости в хранении данных;
— прекращения деятельности Оператора, если иное не предусмотрено законом.

11.2. Бумажные документы уничтожаются путем измельчения, сжигания или иным способом, исключающим восстановление содержащихся в них персональных данных.

11.3. Электронные данные уничтожаются путем удаления из информационных систем, файлов, таблиц, CRM, почты, мессенджеров, облачных хранилищ и иных мест хранения, если их дальнейшее хранение не требуется по закону.

11.4. При невозможности немедленного уничтожения персональные данные блокируются до момента уничтожения.

11.5. Уничтожение персональных данных может фиксироваться актом об уничтожении персональных данных.

12. Ответственное лицо

12.1. Ответственным за организацию обработки и защиты персональных данных является:

ИП Козарезова Маргарита Витальевна

либо иное лицо, назначенное отдельным приказом Оператора:

Козарезова Маргарита Витальевна, руководитель
Ф.И.О., должность

12.2. Ответственное лицо:

— организует обработку и защиту персональных данных;
— контролирует доступ к персональным данным;
— ведет перечень лиц, имеющих доступ к персональным данным;
— организует ознакомление сотрудников и подрядчиков с настоящим Положением;
— контролирует выполнение требований настоящего Положения;
— рассматривает обращения субъектов персональных данных;
— организует уничтожение персональных данных;
— принимает меры при выявлении инцидентов безопасности.

13. Ответственность лиц, имеющих доступ к персональным данным

13.1. Лица, виновные в нарушении требований законодательства Российской Федерации о персональных данных и настоящего Положения, несут ответственность в соответствии с законодательством Российской Федерации, договорами и внутренними документами Оператора.

13.2. Нарушениями считаются:

— незаконный доступ к персональным данным;
— передача персональных данных третьим лицам без разрешения;
— копирование клиентской базы без служебной необходимости;
— использование персональных данных в личных целях;
— публикация фото, видео или иной информации о клиенте без согласия;
— хранение данных в незащищенных местах;
— передача логинов и паролей;
— несообщение об инциденте безопасности;
— иные действия, нарушающие требования настоящего Положения.

14. Заключительные положения

14.1. Настоящее Положение вступает в силу с даты его утверждения Оператором.

14.2. Положение действует бессрочно до его отмены или утверждения новой редакции.

14.3. Изменения в Положение вносятся Оператором при изменении законодательства, состава обрабатываемых персональных данных, используемых информационных систем, порядка доступа к данным или внутренних процессов студии.

14.4. Все лица, имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением.

14.5. Настоящее Положение хранится у Оператора и предоставляется уполномоченным лицам и органам в случаях, предусмотренных законодательством Российской Федерации.

Приложение № 1
к Положению о защите персональных данных

ПЕРЕЧЕНЬ ЛИЦ,
имеющих доступ к персональным данным

№	Ф.И.О.	Должность / роль	К каким данным есть доступ	Информационные системы	Основание доступа	Дата предоставления доступа	Дата прекращения доступа	Подпись
1	Козарцова М.В	ИП / руководитель	Полный доступ	CRM, почта, сайт, документы	Организация деятельности	01.06.26	—	
2		Администратор	Клиенты, записи, абонементы, оплаты, контакты	CRM, онлайн-запись, мессенджеры	Рабочие обязанности			
3		Тренер	ФИО клиента, запись, посещение, ограничения по нагрузке	CRM / расписание	Проведение занятий			
4		Бухгалтер	Данные для учета оплат и документов	Платежный сервис, документы	Бухгалтерский и налоговый учет			
5		Маркетолог / SMM	Заявки, контакты, согласованные материалы	CRM, соцсети, рекламные кабинеты	Реклама и коммуникации			
6		IT-специалист	Технический доступ	Сайт, CRM, хостинг	Техническое сопровождение			

Приложение № 2
к Положению о защите персональных данных

ЖУРНАЛ ПРОВЕРОК
соблюдения требований по защите персональных данных

№	Дата проверки	Что проверялось	Выявленные нарушения	Принятые меры	Ответственное лицо	Срок устранения	Отметка об устранении
1		Доступы к CRM / почте / мессенджерам					
2		Хранение бумажных документов					
3		Наличие согласий клиентов					
4		Доступы сотрудников и подрядчиков					
5		Порядок уничтожения данных					

Приложение № 3
к Положению о защите персональных данных

АКТ
об уничтожении персональных данных

г. Краснодар

«01» июня 2026 г.

Индивидуальный предприниматель Козарезова Маргарита Витальевна составила настоящий акт о том, что были уничтожены персональные данные:

1. Категория персональных данных:
_____

2. Категория субъектов персональных данных:
_____

3. Основание уничтожения:
_____

4. Способ уничтожения:
_____

5. Дата уничтожения:
«___» _____ 20___ г.

6. Ответственное лицо:
_____

Подпись: _____

Приложение № 4
к Положению о защите персональных данных

ЛИСТ ОЗНАКОМЛЕНИЯ
с Положением о защите персональных данных

№	Ф.И.О.	Должность / роль	Дата ознакомления	Подпись
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				