

Политика защиты персональных данных

Для сайта loglaft.ru

Редакция от 17 сентября 2026 года

Документ описывает применяемый оператором подход к обеспечению безопасности персональных данных посетителей сайта, заявителей и клиентов. Он публикуется для информирования пользователей о требованиях и мерах защиты без раскрытия сведений, которые могут снизить безопасность информационных систем.

1 Общие положения

1.1. Настоящая Политика определяет основные требования к защите персональных данных, которые ИП Дубровский Виктор Владимирович получает и обрабатывает при использовании сайта <https://loglaft.ru>, при обращениях пользователей и в ходе договорных отношений.

1.2. Политика разработана с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 01.11.2012 № 1119 и иных применимых нормативных правовых актов.

1.3. Требования Политики применяются к автоматизированной и неавтоматизированной обработке. Конкретный состав мер определяется характером данных, способом обработки, актуальными угрозами, уровнем защищенности информационных систем и требованиями законодательства.

2 Сведения об операторе

Сведения	Значение
Оператор	Индивидуальный предприниматель Дубровский Виктор Владимирович
ИНН	431300046248
ОГРНИП	307431329500058
Адрес регистрации	610007, Кировская область, г. Киров, ул. 65-летия Победы, д. 3
Почтовый адрес	610007, Кировская область, г.о. город Киров, г. Киров, ул. 65-летия Победы, д. 3, кв. 236
Электронная почта	Dubrovskiy.1979@yandex.ru
Сайт	https://loglaft.ru

3 Цели защиты персональных данных

Оператор защищает персональные данные от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения и от иных неправомерных действий.

- сохранение конфиденциальности персональных данных, если закон не предусматривает иное
- обеспечение целостности и доступности данных в пределах, необходимых для законных целей обработки
- предотвращение обработки данных неуполномоченными лицами
- своевременное выявление инцидентов и уменьшение их последствий
- восстановление данных и работоспособности систем после сбоев или инцидентов

4 Организационные меры

Оператор принимает необходимые и достаточные организационные меры с учетом масштаба и характера обработки. К таким мерам относятся:

- назначение лица, ответственного за организацию обработки персональных данных, либо выполнение этих функций оператором лично
- принятие локальных документов, определяющих порядок обработки, доступа, хранения, передачи, блокирования и уничтожения данных
- определение перечня лиц, которым доступ к данным необходим для выполнения обязанностей, и предоставление минимально необходимого объема прав
- ознакомление допущенных лиц с требованиями законодательства и локальных документов, а при необходимости их обучение
- учет носителей и мест хранения данных, если такие носители и места используются
- проверка соблюдения установленных правил и периодическая оценка эффективности мер защиты
- закрепление требований к конфиденциальности и безопасности в договорах с лицами, обрабатывающими данные по поручению оператора

5 Технические меры

Состав технических мер выбирается по результатам оценки угроз и с учетом используемых систем. В применимой части оператор обеспечивает:

- идентификацию и аутентификацию пользователей информационных систем
- разграничение прав доступа и прекращение доступа, когда он больше не требуется
- защиту учетных записей и использование устойчивых паролей
- защиту рабочих устройств, серверов, каналов связи и административных интерфейсов
- применение защищенного соединения HTTPS при передаче данных через сайт
- защиту от вредоносного программного обеспечения и своевременное обновление программных компонентов
- регистрацию значимых событий безопасности и контроль попыток несанкционированного доступа
- резервное копирование и проверку возможности восстановления, когда это необходимо
- удаление или обезличивание данных после достижения целей обработки и истечения обязательных сроков хранения

6 Защита данных на сайте

6.1. Формы сайта должны передавать данные по защищенному соединению. Доступ к заявкам предоставляется только лицам, которым он необходим для обработки обращения пользователя.

6.2. Оператор стремится собирать через формы только данные, необходимые для указанной цели. На момент подготовки настоящей редакции форма консультации на сайте запрашивает имя и номер телефона.

6.3. Аналитические технологии, включая Яндекс Метрику, должны активироваться с учетом выбранных пользователем настроек cookie. Сведения о составе cookie и порядке управления ими приводятся в отдельном согласии на сбор и обработку файлов cookie.

6.4. На страницах сбора персональных данных пользователю должен быть доступен текст Политики обработки персональных данных и отдельный элемент для выражения согласия, когда согласие является правовым основанием обработки.

7 Привлечение третьих лиц

7.1. Если обработка поручается другому лицу, оператор определяет перечень данных, действия с ними, цели обработки, требования к конфиденциальности, безопасности и подтверждению принятых мер.

7.2. Оператор оценивает поставщиков услуг, имеющих доступ к персональным данным, и ограничивает такой доступ объемом, необходимым для оказания соответствующей услуги.

7.3. Использование внешнего сервиса не освобождает оператора от обязанностей перед субъектами персональных данных.

8 Выявление и устранение инцидентов

8.1. Лицо, обнаружившее признаки утечки, неправомерного доступа, уничтожения, изменения или блокирования данных, должно без промедления сообщить об этом ответственному лицу или оператору.

8.2. Оператор ограничивает дальнейший доступ, сохраняет необходимые сведения о событии, оценивает затронутые данные и лиц, устраняет причины инцидента и принимает меры для предупреждения повторения.

8.3. При установлении факта неправомерной или случайной передачи персональных данных, повлекшей нарушение прав субъектов, оператор направляет в Роскомнадзор первоначальное уведомление в течение 24 часов и результаты внутреннего расследования в течение 72 часов, если иной порядок не установлен законом.

9 Уничтожение и восстановление данных

9.1. Данные уничтожаются либо обезличиваются при достижении целей обработки, утрате необходимости в их достижении, истечении срока согласия, отзыве согласия, выявлении неправомерной обработки или наступлении иного предусмотренного законом основания.

9.2. Уничтожение выполняется способом, исключающим восстановление содержания данных штатными средствами. Если немедленное уничтожение невозможно, данные блокируются на срок, необходимый для завершения уничтожения.

9.3. Резервные копии используются только для восстановления работоспособности и защищаются не слабее основных данных. Сведения из резервных копий удаляются по установленному циклу обновления копий.

10 Контроль и пересмотр

Оператор пересматривает Политику при изменении законодательства, состава обрабатываемых данных, информационных систем, используемых сервисов или выявленных угроз. Актуальная редакция публикуется на сайте и действует со дня публикации, если в ней не указан иной срок.

11 Обращения по вопросам защиты данных

Сообщения о возможных нарушениях и запросы по вопросам защиты персональных данных можно направить по адресу электронной почты Dubrovskiy.1979@yandex.ru или по почтовому адресу: 610007, Кировская область, г.о. город Киров, г. Киров, ул. 65-летия Победы, д. 3, кв. 236.