Рекомендации по соответствию законодательству РФ

Версия документа: 1.0
Дата: 2025-11-30
Применимость: Telegram Store MVP для российского рынка

Содержание

Обзор регуляторных требований

Основные законы и нормативные акты

Закон/НПА	Описание	Применимость к проекту
152-ФЗ	О персональных данных	✅ Обязательно (сбор ФИО, телефона, адреса)
54-ФЗ	О применении ККТ	⚠️ Фаза 2 (при внедрении онлайн-платежей)
149-ФЗ	Об информации, информационных технологиях	✅ Обязательно (хранение данных в РФ)
2300-1	О защите прав потребителей	✅ Обязательно (розничная торговля)
Приказ ФСТЭК №21	Требования к защите ПДн	✅ Обязательно (технические меры)

Ответственность за нарушения

Нарушение	Штраф для ИП	Штраф для юр. лиц	Статья КоАП
Обработка ПДн без согласия	10-20 тыс. руб.	30-50 тыс. руб.	13.11 ч.2
Нарушение требований к защите ПДн	10-20 тыс. руб.	30-75 тыс. руб.	13.11 ч.1
Хранение данных вне РФ	30-50 тыс. руб.	100-300 тыс. руб.	13.11 ч.8
Неприменение ККТ	25-50% от суммы	75-100% от суммы	14.5

152-ФЗ “О персональных данных”

Что является персональными данными в проекте

Собираемые ПДн:
- ✅ ФИО клиента
- ✅ Номер телефона
- ✅ Адрес доставки
- ✅ Telegram User ID (может быть ПДн в контексте)
- ✅ Telegram Username (если указан)
- ⚠️ История заказов (косвенно идентифицирует)

НЕ являются ПДн:
- ❌ Информация о продуктах
- ❌ Цены
- ❌ Статусы заказов (без привязки к личности)

Требования к обработке ПДн

1. Получение согласия

Обязательно:
- [ ] Явное согласие пользователя ДО сбора данных
- [ ] Информирование о целях обработки
- [ ] Информирование о составе данных
- [ ] Информирование о сроках хранения
- [ ] Возможность отозвать согласие

Пример реализации в Telegram Bot:

```
# При первом запуске бота
@router.message(Command("start"))
async def cmd_start(message: Message, state: FSMContext):
    await message.answer(
        "👋 Добро пожаловать в наш магазин!\n\n"
        "Для оформления заказа нам потребуется собрать ваши персональные данные "
        "(ФИО, телефон, адрес доставки).\n\n"
        "📄 Ознакомьтесь с нашей Политикой конфиденциальности: "
        "https://telegram-shop.example/privacy\n\n"
        "Продолжая использование бота, вы соглашаетесь на обработку ваших "
        "персональных данных в соответствии с 152-ФЗ.",
        reply_markup=get_consent_keyboard()
    )

def get_consent_keyboard():
    return InlineKeyboardMarkup(inline_keyboard=[
        [InlineKeyboardButton(text="✅ Согласен", callback_data="consent_agree")],
        [InlineKeyboardButton(text="❌ Не согласен", callback_data="consent_decline")]
,
        [InlineKeyboardButton(text="📄 Политика конфиденциальности",
                              url="https://telegram-shop.example/privacy")]
    ])

@router.callback_query(F.data == "consent_agree")
async def consent_agreed(callback: CallbackQuery, state: FSMContext):
    # Сохранить согласие в БД с timestamp
    await save_user_consent(callback.from_user.id, agreed=True)
    await callback.message.edit_text("✅ Спасибо! Теперь вы можете пользоваться
магазином.")
    await show_main_menu(callback.message)
```

2. Цели обработки

Законные цели для проекта:

- ✅ Исполнение договора купли-продажи (оформление и доставка заказа)
- ✅ Связь с клиентом по вопросам заказа
- ✅ Улучшение качества обслуживания
- ❌ Маркетинг и рассылки (требуется отдельное согласие)

Важно: Нельзя использовать данные для целей, не указанных при получении согласия.

3. Уровни защищенности ПДн

Определение уровня:

Для проекта применяется **УЗ-2** (2-й уровень защищенности):

- Обрабатываются общедоступные ПДн (ФИО, телефон, адрес)
- Количество субъектов: до 100,000
- Актуальная угроза: средняя
- Не обрабатываются биометрические, специальные категории ПДн

Требования УЗ-2:

Требование	Реализация в проекте
Идентификация и аутентификация	JWT для админов, Telegram ID для клиентов
Управление доступом	RBAC в Admin Panel
Регистрация событий	Логирование всех операций с ПДн
Антивирусная защита	ClamAV на сервере
Обнаружение вторжений	Fail2ban, IDS
Контроль целостности	Checksums для критичных файлов
Резервное копирование	Ежедневные backup
Шифрование	TLS для передачи, AES-256 для хранения

4. Технические меры защиты

Обязательные меры:

```
# Шифрование персональных данных в БД
Encryption:
  - Algorithm: AES-256-GCM
  - Key Management: AWS KMS / HashiCorp Vault
  - Fields: phone_number, shipping_address, full_name

# Пример с SQLAlchemy
from sqlalchemy_utils import EncryptedType
from sqlalchemy_utils.types.encrypted.encrypted_type import AesEngine

class User(Base):
    __tablename__ = "users"

    id = Column(BigInteger, primary_key=True)
    full_name = Column(EncryptedType(String,
                                     settings.ENCRYPTION_KEY,
                                     AesEngine, 'pkcs5'))
    phone_number = Column(EncryptedType(String,
                                        settings.ENCRYPTION_KEY,
                                        AesEngine, 'pkcs5'))
    # ...
```

Контроль доступа:

```python
# Логирование доступа к ПДн
import logging

audit_logger = logging.getLogger('audit')

async def get_user_personal_data(user_id: int, admin_id: int):
    # Логирование доступа
    audit_logger.info(
        f"PERSONAL_DATA_ACCESS: admin_id={admin_id} accessed user_id={user_id} data",
        extra={
            "event_type": "pdn_access",
            "admin_id": admin_id,
            "user_id": user_id,
            "timestamp": datetime.utcnow().isoformat()
        }
    )

    # Получение данных
    user = await db.query(User).filter(User.id == user_id).first()
    return user
```

54-ФЗ “О применении ККТ” (онлайн-кассы)

Когда требуется ККТ

Обязательно для MVP: ❌ НЕТ (если нет онлайн-платежей)

Обязательно для Фазы 2: ✅ ДА (при внедрении онлайн-оплаты)

Требования 54-ФЗ

При приеме онлайн-платежей:

- [ ] Использование онлайн-кассы с фискальным накопителем
- [ ] Регистрация ККТ в ФНС
- [ ] Договор с ОФД (Оператор Фискальных Данных)
- [ ] Отправка чека клиенту (email или SMS)
- [ ] Передача данных в ФНС в реальном времени

Интеграция с ОФД (для Фазы 2)

Популярные ОФД:

- АТОЛ Онлайн
- Платформа ОФД
- Такском
- Эвотор

Пример интеграции с АТОЛ:

```python
import requests

class AtolFiscalization:
    def __init__(self, login: str, password: str, group_code: str):
        self.base_url = "https://online.atol.ru/possystem/v4"
        self.login = login
        self.password = password
        self.group_code = group_code
        self.token = None

    async def get_token(self):
        response = requests.post(
            f"{self.base_url}/getToken",
            json={"login": self.login, "pass": self.password}
        )
        self.token = response.json()["token"]

    async def create_receipt(self, order: Order):
        receipt_data = {
            "external_id": str(order.id),
            "receipt": {
                "client": {
                    "email": order.customer_email,
                    "phone": order.customer_phone
                },
                "company": {
                    "email": "shop@example.com",
                    "sno": "usn_income",  # Система налогообложения
                    "inn": "1234567890",
                    "payment_address": "https://telegram-shop.example"
                },
                "items": [
                    {
                        "name": item.product_name,
                        "price": float(item.price),
                        "quantity": item.quantity,
                        "sum": float(item.price * item.quantity),
                        "tax": "vat20",  # НДС 20%
                        "payment_method": "full_payment",
                        "payment_object": "commodity"
                    }
                    for item in order.items
                ],
                "payments": [
                    {
                        "type": 1,  # Электронный платеж
                        "sum": float(order.total_amount)
                    }
                ],
                "total": float(order.total_amount)
            }
        }

        response = requests.post(
            f"{self.base_url}/{self.group_code}/sell",
            headers={"Token": self.token},
            json=receipt_data
        )

        return response.json()
```

Штрафы за неприменение ККТ

- **Для ИП:** 25-50% от суммы расчета (минимум 10,000 руб.)
- **Для юр. лиц:** 75-100% от суммы расчета (минимум 30,000 руб.)
- **Повторное нарушение:** приостановление деятельности до 90 дней

Локализация данных

Требования 152-ФЗ (ст. 18, п. 5)

Обязательно:
- ✅ Запись, систематизация, накопление, хранение, уточнение, извлечение ПДн граждан РФ должны осуществляться с использованием баз данных, находящихся на территории РФ

Что это значит:
- Серверы с PostgreSQL должны быть физически в России
- Backup также должны храниться в РФ
- Допускается трансграничная передача (например, в Google Analytics), но первичное хранение - в РФ

Проверка локализации

Как убедиться:

```
# Проверка IP адреса сервера
curl ifconfig.me

# Проверка геолокации IP
curl https://ipapi.co/$(curl -s ifconfig.me)/country/
# Должно вернуть: RU

# Проверка через whois
whois $(curl -s ifconfig.me) | grep -i country
```

Рекомендуемые хостинг-провайдеры в РФ

Провайдер	Дата-центры	Сертификация	Цена (от)
Yandex Cloud	Москва, Владимир	152-ФЗ, ISO 27001	~3000₽/мес
VK Cloud (MCS)	Москва	152-ФЗ, ISO 27001	~2500₽/мес
Selectel	Москва, СПб	152-ФЗ, PCI DSS	~2000₽/мес
Timeweb Cloud	Москва	152-ФЗ	~1500₽/мес
REG.RU	Москва	152-ФЗ	~1000₽/мес

Важно: Выбирайте провайдера с сертификацией соответствия 152-ФЗ.

Политика конфиденциальности

Обязательные разделы

Политика конфиденциальности должна содержать:

1. **Оператор ПДн** - наименование, ИНН, адрес, контакты
2. **Цели обработки** - для чего собираются данные
3. **Состав ПДн** - какие именно данные собираются
4. **Правовые основания** - согласие, договор, законные интересы
5. **Сроки хранения** - как долго хранятся данные
6. **Права субъекта** - доступ, исправление, удаление
7. **Меры защиты** - технические и организационные меры
8. **Передача третьим лицам** - кому и на каких основаниях
9. **Трансграничная передача** - если есть (Google Analytics, Yandex Metrika)
10. **Контакты** - как связаться по вопросам ПДн

Шаблон Политики конфиденциальности

```
# ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ

**Дата вступления в силу:** 01.12.2025

## 1. Общие положения

Настоящая Политика конфиденциальности (далее – Политика) определяет порядок
обработки и защиты персональных данных пользователей Telegram-бота
"[Название магазина]" (далее – Сервис).

**Оператор персональных данных:**
- Наименование: ИП Иванов Иван Иванович / ООО "Название"
- ИНН: 1234567890
- ОГРН/ОГРНИП: 1234567890123
- Адрес: 123456, г. Москва, ул. Примерная, д. 1
- Email: privacy@telegram-shop.example
- Телефон: +7 (999) 123-45-67

## 2. Какие данные мы собираем

При использовании Сервиса мы собираем следующие персональные данные:
- ФИО (для оформления заказа)
- Номер телефона (для связи по заказу)
- Адрес доставки (для доставки товара)
- Telegram User ID (для идентификации в системе)
- Telegram Username (если указан в профиле)
- История заказов (для учета и аналитики)

## 3. Цели обработки данных

Мы обрабатываем ваши персональные данные для следующих целей:
- Исполнение договора купли-продажи (оформление и доставка заказа)
- Связь с вами по вопросам заказа
- Улучшение качества обслуживания
- Соблюдение требований законодательства РФ

## 4. Правовые основания

Обработка персональных данных осуществляется на основании:
- Вашего согласия (ст. 9 152-ФЗ)
- Необходимости исполнения договора (п. 5 ч. 1 ст. 6 152-ФЗ)

## 5. Сроки хранения

Ваши персональные данные хранятся:
- В течение срока действия договора
- 5 лет после последнего заказа (для бухгалтерского учета)
- До момента отзыва согласия (если применимо)

## 6. Ваши права

Вы имеете право:
- Получить информацию о ваших персональных данных
- Требовать исправления неточных данных
- Требовать удаления данных (право на забвение)
- Отозвать согласие на обработку
- Обжаловать действия оператора в Роскомнадзоре

Для реализации прав напишите на: privacy@telegram-shop.example

## 7. Меры защиты
```

```
Мы применяем следующие меры защиты:
- Шифрование данных при передаче (TLS 1.2+)
- Шифрование данных при хранении (AES-256)
- Контроль доступа (только уполномоченные лица)
- Регулярное резервное копирование
- Мониторинг безопасности

## 8. Передача третьим лицам

Мы можем передавать ваши данные:
- Службам доставки (для доставки заказа)
- Платежным системам (для обработки платежей) - Фаза 2
- Google Analytics, Yandex Metrika (анонимизированная аналитика)

Мы НЕ продаем ваши данные третьим лицам.

## 9. Трансграничная передача

Данные могут передаваться за пределы РФ:
- Google Analytics (США) - для аналитики
- Yandex Metrika (Россия) - для аналитики

Первичное хранение данных осуществляется на серверах в РФ.

## 10. Cookies и аналитика

Мы используем cookies и аналитические системы для:
- Улучшения работы Сервиса
- Анализа поведения пользователей
- Персонализации контента

Вы можете отключить cookies в настройках браузера.

## 11. Изменения Политики

Мы можем обновлять Политику. Актуальная версия всегда доступна по адресу:
https://telegram-shop.example/privacy

При существенных изменениях мы уведомим вас через Telegram-бот.

## 12. Контакты

По вопросам обработки персональных данных:
- Email: privacy@telegram-shop.example
- Telegram: @shop_support_bot
- Телефон: +7 (999) 123-45-67

**Дата последнего обновления:** 01.12.2025
```

Где разместить Политику

- [ ] На отдельной странице сайта (https://telegram-shop.example/privacy)
- [ ] Ссылка в Telegram Bot (команда /privacy)
- [ ] В Admin Panel (футер)
- [ ] При первом запуске бота (согласие)

Пользовательское соглашение

Отличие от Политики конфиденциальности

Документ	Регулирует	Обязательность
Политика конфиденциальности	Обработку ПДн	✅ Обязательно (152-ФЗ)
Пользовательское соглашение	Правила использования сервиса	⚠️ Рекомендуется (ГК РФ)

Обязательные разделы Пользовательского соглашения

1. **Предмет соглашения** - что предоставляет сервис
2. **Регистрация и аккаунт** - правила использования
3. **Права и обязанности сторон**
4. **Оплата и доставка** - условия покупки
5. **Возврат и обмен** - в соответствии с Законом о ЗПП
6. **Ответственность сторон**
7. **Разрешение споров**
8. **Заключительные положения**

Краткий шаблон

```
# ПОЛЬЗОВАТЕЛЬСКОЕ СОГЛАШЕНИЕ

## 1. Общие положения

Настоящее Соглашение регулирует отношения между Продавцом и Покупателем
при использовании Telegram-бота "[Название магазина]".

Используя Сервис, вы соглашаетесь с условиями настоящего Соглашения.

## 2. Оформление заказа

2.1. Покупатель оформляет заказ через Telegram-бот.
2.2. Заказ считается принятым после подтверждения Продавцом.
2.3. Продавец вправе отказать в исполнении заказа при отсутствии товара.

## 3. Оплата

3.1. Оплата производится [наличными при получении / онлайн].
3.2. Цены указаны в рублях РФ с учетом НДС.

## 4. Доставка

4.1. Доставка осуществляется по адресу, указанному Покупателем.
4.2. Сроки доставки: [указать сроки].
4.3. Стоимость доставки: [указать условия].

## 5. Возврат и обмен

5.1. Возврат товара надлежащего качества - в течение 7 дней.
5.2. Возврат товара ненадлежащего качества - в течение гарантийного срока.
5.3. Условия возврата регулируются Законом РФ "О защите прав потребителей".

## 6. Ответственность

6.1. Продавец не несет ответственности за задержки доставки по вине
      курьерской службы.
6.2. Покупатель несет ответственность за достоверность предоставленных данных.

## 7. Разрешение споров

7.1. Споры разрешаются путем переговоров.
7.2. При недостижении согласия - в суде по месту нахождения Продавца.

## 8. Контакты

Email: support@telegram-shop.example
Телефон: +7 (999) 123-45-67
```

Права пользователей

Права субъекта ПДн (152-ФЗ, ст. 14)

Пользователь имеет право:

1. **На доступ к своим данным**
   - Получить информацию о том, какие данные обрабатываются
   - Получить копию своих данных

2. **На исправление**
   - Потребовать исправления неточных данных
   - Дополнить неполные данные

3. **На удаление (право на забвение)**
   - Потребовать удаления данных при отзыве согласия
   - Потребовать удаления при достижении целей обработки

4. **На ограничение обработки**
   - Ограничить обработку на период проверки точности данных

5. **На отзыв согласия**
   - Отозвать согласие в любой момент

6. **На обжалование**
   - Обжаловать действия оператора в Роскомнадзоре или суде

Реализация прав в проекте

Команда /my_data в Telegram Bot:

```
@router.message(Command("my_data"))
async def cmd_my_data(message: Message):
    user = await get_user(message.from_user.id)

    if not user:
        await message.answer("У нас нет ваших данных.")
        return

    data_text = f"""
📋 **Ваши персональные данные:**

ФИО: {user.full_name}
Телефон: {user.phone_number}
Telegram ID: {user.id}
Username: @{user.username or 'не указан'}
Дата регистрации: {user.created_at.strftime('%d.%m.%Y')}

📊 **Статистика:**
Всего заказов: {await get_orders_count(user.id)}

🔧 **Управление данными:**
/edit_data - Изменить данные
/delete_data - Удалить все данные
/export_data - Экспортировать данные (JSON)
    """

    await message.answer(data_text, parse_mode="Markdown")

@router.message(Command("delete_data"))
async def cmd_delete_data(message: Message):
    await message.answer(
        "⚠️ Вы уверены, что хотите удалить все свои данные?\n\n"
        "Это действие необратимо. Вся история заказов будет удалена.",
        reply_markup=InlineKeyboardMarkup(inline_keyboard=[
            [InlineKeyboardButton(text="✅ Да, удалить",
                                  callback_data="confirm_delete_data")],
            [InlineKeyboardButton(text="❌ Отмена",
                                  callback_data="cancel_delete_data")]
        ])
    )

@router.callback_query(F.data == "confirm_delete_data")
async def confirm_delete(callback: CallbackQuery):
    # Удаление данных (GDPR right to be forgotten)
    await delete_user_data(callback.from_user.id)

    # Логирование для аудита
    audit_logger.info(
        f"USER_DATA_DELETED: user_id={callback.from_user.id}",
        extra={"event_type": "data_deletion", "user_id": callback.from_user.id}
    )

    await callback.message.edit_text(
        "✅ Ваши данные успешно удалены.\n\n"
        "Для повторного использования бота нажмите /start"
    )

@router.message(Command("export_data"))
async def cmd_export_data(message: Message):
    user_data = await get_user_full_data(message.from_user.id)

    # Формирование JSON
```

```
    export_json = json.dumps(user_data, ensure_ascii=False, indent=2)

    # Отправка файла
    file = BufferedInputFile(
        export_json.encode('utf-8'),
        filename=f"my_data_{message.from_user.id}.json"
    )

    await message.answer_document(
        file,
        caption="📄 Ваши персональные данные в формате JSON"
    )
```

Шифрование и защита данных

Требования к шифрованию

Приказ ФСТЭК №21 (для УЗ-2):
- ✅ Шифрование при передаче (TLS 1.2+)
- ✅ Шифрование при хранении (рекомендуется для ПДн)
- ✅ Использование сертифицированных средств (для гостайны, для коммерческих данных - рекомендация)

Реализация шифрования

1. Шифрование при передаче:

```
# Nginx SSL конфигурация
ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256';
ssl_prefer_server_ciphers on;
```

2. Шифрование при хранении:

```python
# Шифрование полей в PostgreSQL
from cryptography.fernet import Fernet
import base64

class EncryptedField:
    def __init__(self, key: bytes):
        self.cipher = Fernet(key)

    def encrypt(self, value: str) -> str:
        return self.cipher.encrypt(value.encode()).decode()

    def decrypt(self, value: str) -> str:
        return self.cipher.decrypt(value.encode()).decode()

# Использование
encryption_key = base64.urlsafe_b64encode(settings.ENCRYPTION_KEY.encode())
encryptor = EncryptedField(encryption_key)

# При сохранении
user.phone_number = encryptor.encrypt("+79991234567")

# При чтении
phone = encryptor.decrypt(user.phone_number)
```

3. Шифрование backup:

```bash
# GPG шифрование backup
gpg --encrypt --recipient admin@example.com backup.sql.gz

# Расшифровка
gpg --decrypt backup.sql.gz.gpg > backup.sql.gz
```

Сроки хранения данных

Законодательные требования

Тип данных	Минимальный срок	Основание
Бухгалтерские документы	5 лет	ФЗ-402 “О бухучете”
Кассовые документы	5 лет	ФЗ-54 “О ККТ”
Договоры	5 лет	ГК РФ
Персональные данные	До достижения цели или отзыва согласия	152-ФЗ

Рекомендуемые сроки для проекта

```python
# Конфигурация сроков хранения
DATA_RETENTION_POLICY = {
    "active_users": None,  # Бессрочно, пока пользуется
    "inactive_users": 365 * 3,  # 3 года после последней активности
    "completed_orders": 365 * 5,  # 5 лет (бухгалтерия)
    "cancelled_orders": 365 * 1,  # 1 год
    "logs": 90,  # 90 дней
    "audit_logs": 365 * 3,  # 3 года
}

# Автоматическая очистка (cron job)
async def cleanup_old_data():
    # Удаление неактивных пользователей
    inactive_threshold = datetime.now() - timedelta(
        days=DATA_RETENTION_POLICY["inactive_users"]
    )

    await db.execute(
        delete(User).where(
            and_(
                User.last_activity < inactive_threshold,
                User.consent_withdrawn == True
            )
        )
    )

    # Удаление старых логов
    log_threshold = datetime.now() - timedelta(
        days=DATA_RETENTION_POLICY["logs"]
    )

    # Очистка файлов логов старше 90 дней
    # ...
```

Уведомление Роскомнадзора

Когда требуется уведомление

Обязательно уведомлять Роскомнадзор:
- ✅ При начале обработки ПДн (до начала обработки)
- ✅ При изменении сведений об операторе
- ✅ При прекращении обработки ПДн

Исключения (можно не уведомлять):
- ❌ Если обрабатываются только данные сотрудников (трудовые отношения)
- ❌ Если оператор - физлицо для личных нужд

Для проекта: ✅ Уведомление ОБЯЗАТЕЛЬНО (обработка данных клиентов)

Как уведомить

Способы подачи уведомления:

1. **Онлайн** - через личный кабинет на сайте Роскомнадзора (https://pd.rkn.gov.ru/)

2. **Почтой** - заказным письмом в территориальное управление
3. **Лично** - в территориальном управлении

Необходимые документы:
- [ ] Уведомление об обработке ПДн (форма утверждена Приказом №996)
- [ ] Копия ОГРН/ОГРНИП
- [ ] Копия ИНН
- [ ] Доверенность (если подает представитель)

Сроки:
- Подать уведомление: до начала обработки ПДн
- Рассмотрение: в течение 30 дней
- Регистрация в реестре: после рассмотрения

Штрафы за неуведомление

- **Для ИП:** 3,000 - 5,000 руб.
- **Для юр. лиц:** 30,000 - 50,000 руб.

Чеклист соответствия

Перед запуском MVP

152-ФЗ “О персональных данных”

- [ ] Серверы расположены на территории РФ
- [ ] Политика конфиденциальности разработана и опубликована
- [ ] Механизм получения согласия реализован в боте
- [ ] Шифрование ПДн при хранении настроено
- [ ] TLS 1.2+ для передачи данных
- [ ] Логирование доступа к ПДн настроено
- [ ] Права пользователей реализованы (/my_data, /delete_data)
- [ ] Уведомление Роскомнадзора подано
- [ ] Назначен ответственный за обработку ПДн
- [ ] Разработаны внутренние документы (Положение об обработке ПДн)

Закон “О защите прав потребителей”

- [ ] Пользовательское соглашение разработано
- [ ] Информация о продавце доступна (ИНН, адрес, контакты)
- [ ] Условия возврата и обмена указаны
- [ ] Сроки доставки указаны
- [ ] Гарантийные обязательства описаны

Техническая защита

- [ ] Firewall настроен
- [ ] Антивирус установлен
- [ ] IDS/IPS настроен
- [ ] Backup автоматизирован
- [ ] Мониторинг безопасности настроен

- [ ] Incident response plan разработан

Перед запуском Фазы 2 (онлайн-платежи)

54-ФЗ “О применении ККТ”

- [ ] Онлайн-касса приобретена и зарегистрирована в ФНС
- [ ] Договор с ОФД заключен
- [ ] Интеграция с ОФД реализована
- [ ] Отправка чеков клиентам настроена
- [ ] Тестирование фискализации проведено

PCI DSS (если обрабатываются карты)

- [ ] Не хранить CVV/CVC
- [ ] Использовать токенизацию (через payment gateway)
- [ ] Шифрование всех платежных данных
- [ ] Регулярные security аудиты

Полезные ресурсы

Официальные источники

- **Роскомнадзор:** https://rkn.gov.ru/
- **Личный кабинет оператора ПДн:** https://pd.rkn.gov.ru/
- **ФНС (онлайн-кассы):** https://www.nalog.gov.ru/rn77/taxation/kkt/
- **Консультант Плюс (законы):** http://www.consultant.ru/

Тексты законов

- **152-ФЗ:** http://www.consultant.ru/document/cons_doc_LAW_61801/
- **54-ФЗ:** http://www.consultant.ru/document/cons_doc_LAW_42359/
- **149-ФЗ:** http://www.consultant.ru/document/cons_doc_LAW_61798/
- **Закон о ЗПП:** http://www.consultant.ru/document/cons_doc_LAW_305/

Методические материалы

- **Роскомнадзор - Разъяснения по 152-ФЗ:** https://rkn.gov.ru/personal-data/
- **ФСТЭК - Требования к защите ПДн:** https://fstec.ru/
- **Приказ ФСТЭК №21:** https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21

Контакты для консультаций

Юридическая поддержка

- **Роскомнадзор горячая линия:** 8-800-707-77-07
- **ФНС консультации:** 8-800-222-22-22

Рекомендуемые юристы (специализация: IT, ПДн)

- Консультация с юристом по 152-ФЗ перед запуском

- Аудит документов (Политика, Соглашение)
- Сопровождение при уведомлении Роскомнадзора

Версия: 1.0
Последнее обновление: 2025-11-30
Ответственный: Legal / Compliance Officer

Disclaimer: Данный документ носит рекомендательный характер и не является юридической консультацией. Для точной оценки соответствия законодательству рекомендуется обратиться к квалифицированному юристу.