

# GeekSTunnel: Licensing, Ethics & Legal Compliance Guide

## 1. Tech Stack Licensing Review

All the core technologies used in GeekSTunnel are **Open Source** and widely accepted for commercial use. You do **not** need to pay any licensing fees to use these underlying components.

Component	License	Commercial Use?
<b>FastAPI</b>	MIT	Yes (Permissive)
<b>WireGuard</b>	GPLv2 (Kernel)	Yes (Standard usage is free)
<b>CoreDNS</b>	Apache 2.0	Yes (Permissive)
<b>Nginx / OpenResty</b>	BSD-style	Yes (Permissive)
<b>MySQL / MariaDB</b>	GPL	Yes (Standard usage is free)
<b>Redis</b>	BSD 3-Clause	Yes (Permissive)
<b>Python Libraries</b>	MIT / BSD	Yes (Permissive)

---

## 2. Ethical Considerations

### 2.1 Intended Use

GeekSTunnel is designed as a **Security & Privacy Tool**. - **Ethical**: Using it for secure remote work, protecting personal privacy on public Wi-Fi, and implementing parental/organizational DNS filtering. - **Unethical**: Using it to facilitate illegal activities, unauthorized data exfiltration, or bypassing critical national security infrastructure.

### 2.2 The “Anti-Bypass” Feature

- **Ethics**: While technically aggressive, this feature is ethically sound when used for **Network Integrity**. It ensures that security policies (like blocking malware or phishing sites) cannot be bypassed by malicious actors or unauthorized software.

---

## 3. Legal Compliance

### 3.1 VPN Legality

VPNs are legal in the vast majority of countries. However, some regions (e.g., China, Russia, UAE, Iran) have specific regulations or licensing requirements for VPN providers. - **Action**: If you plan to sell this as a service in those regions, you should consult with a local legal expert.

### 3.2 Data Privacy (GDPR/CCPA)

Because GeekSTunnel can log user activity (Audit Logs), you must be transparent with your users. - **Action:** If selling as a service, provide a **Privacy Policy** that explains what data is logged and for how long.

---

## 4. How to License YOUR Code

You own the code we have built together. You have three main options for licensing it:

### Option A: Proprietary (Closed Source)

- **Strategy:** You keep the source code secret and sell it as a finished product.
- **Best for:** Selling to enterprises or launching a private SaaS.
- **Cost:** \$0. You just add a LICENSE file stating “All Rights Reserved.”

### Option B: MIT / Apache (Open Source)

- **Strategy:** You allow anyone to use, modify, and sell your code.
- **Best for:** Building a community and gaining fame as a developer.
- **Cost:** \$0.

### Option C: GPL (Copyleft)

- **Strategy:** You allow others to use the code, but they **must** also keep their version open source.
  - **Best for:** Ensuring the code remains free for everyone forever.
- 

## 5. Summary of Charges

- **Software Licenses: \$0** (All underlying tech is free).
- **Hosting (VPS):** You only pay for the server (e.g., DigitalOcean, AWS, Hetzner).
- **Domain:** Standard annual fee for your .com or .online domain.

**Verdict:** You are ethically and legally on solid ground. You have built a professional security tool using the world’s best open-source foundations.