Cybersecurity & compliance checklist for CPOs

Security and compliance are the foundation of a reliable charging network. Use this checklist to evaluate whether your current or future platform partner is secure, compliant, and built for growth.

1. Certifications & trust marks

- ☐ Holds ISO 27001 certification (global benchmark for information security)
- ☐ AFIR compliant for European interoperability
- ☐ Eichrecht certified to guarantee accurate, tamper-proof billing
- ☐ Independent yearly audits for security and finance
- ☐ Meets privacy regulations (GDPR, CCPA, APPI)

2. Data protection

- ☐ All sensitive data is encrypted and backed up securely
- ☐ Customer data is kept separate and private
- ☐ Clear process for reporting and handling data breaches

3. Platform reliability

- ☐ Guaranteed uptime (99% or higher)
- ☐ DDoS protection and failover mechanisms to prevent outages
- ☐ 24/7 monitoring with proactive problem resolution

4. Operational security

- ☐ Regular security testing and system updates
- ☐ Full audit trail of activities for transparency
- ☐ Access managed with role-based permissions and multi-factor login

5. Transaction & payment security

- ☐ Secure communication between charge points and the platform
- ☐ Protection against tampering of energy and billing data
- ☐ Safe handling of all financial transactions
- ☐ Financial transactions encrypted and compliant with AFIR/DSS

6. Ecosystem & vendor security

- ☐ Annual vendor security reviews and due diligence
- ☐ Automated security updates and patching
- ☐ Customer data anonymised when aggregated

7. Scalability

- ☐ Cloud infrastructure with redundancy for resilience
- ☐ Provider-agnostic design (to adapt to new regulations and standards)
- ☐ Built-in tools to support large-scale growth

To learn how Road can support your charging operations with enterprise-grade security and compliance, contact our team today.