

Smart Lock Compliance Checklist

GDPR, ADA, Fire Safety & Industry Standards - 2025 Edition

 LEGAL NOTICE

This checklist provides general guidance only. Requirements vary by jurisdiction. Consult qualified legal counsel and local authorities.

Property: _____ Date: _____

Compliance Officer: _____

 1. Data Privacy & Security (GDPR/CCPA)

- ☐ Privacy policy updated to disclose smart lock data collection
- ☐ Guest consent obtained for data processing
- ☐ Data retention periods defined (max 30 days recommended)
- ☐ Guest right to access personal data documented
- ☐ Guest right to erasure process established
- ☐ Data encrypted at rest (AES-256) and in transit (TLS 1.2+)
- ☐ Data breach notification procedures (72-hour requirement)
- ☐ Data Processing Agreement signed with vendor
- ☐ Staff trained on data privacy (annual training)
- ☐ Data stored in required jurisdictions

 2. Accessibility (ADA Compliance)

- ☐ Lock operation force ≤ 5 lbf (22.2 N)
- ☐ Handle height 34-48 inches from floor
- ☐ Alternative access method available
- ☐ Visual indicators with high color contrast
- ☐ Audio feedback available for blind guests
- ☐ Instructions in accessible formats (large print, Braille)
- ☐ Emergency override accessible without excessive force
- ☐ Key encoding stations accessible (30" max height)

3. Fire & Life Safety

- ☐ Fail-safe egress: Lock unlocks from inside without key
- ☐ No electronic delay on egress (instant exit)
- ☐ Lock unlocks automatically on fire alarm activation
- ☐ Fire personnel emergency override available
- ☐ Fire-rated doors maintain rating after installation
- ☐ UL 294 certification for access control units
- ☐ Local fire marshal approval obtained
- ☐ Emergency power backup tested
- ☐ Fire evacuation procedures updated

4. Building & Safety Codes

- ☐ ANSI/BHMA A156.13 certification (Grade 1 for hotels)
- ☐ Local building code requirements met
- ☐ Door preparation maintains structural integrity
- ☐ Electrical safety standards met
- ☐ FCC Part 15 certification (RF compliance)
- ☐ CE marking (if applicable in jurisdiction)
- ☐ Seismic requirements met (earthquake zones)
- ☐ Hurricane impact standards (coastal properties)

5. Cybersecurity & PCI DSS

- ☐ PCI DSS compliance (if storing payment card data)
- ☐ Network segmentation (locks on isolated VLAN)
- ☐ Default passwords changed on all devices
- ☐ Vendor security patch management process
- ☐ Access control based on need-to-know
- ☐ Audit trails reviewed regularly (weekly minimum)
- ☐ Penetration testing conducted annually

6. Industry Standards

- ☐ ISO/IEC 27001 Information Security Management
- ☐ ISO/IEC 27701 Privacy Information Management
- ☐ NFPA 101 Life Safety Code compliance
- ☐ UL 1034 Burglary-Resistant Electric Locks
- ☐ HTNG hospitality technology standards

7. Insurance & Liability

- ☐ System meets insurer security requirements
- ☐ Certificate of insurance from installer/vendor
- ☐ Product liability coverage verified (\$1M+ recommended)
- ☐ Cyber liability insurance updated for IoT devices
- ☐ Installation complies with insurance policy terms

8. Documentation & Records

- ☐ Installation certificates on file (3-7 year retention)
- ☐ Inspection reports documented (annual minimum)
- ☐ Maintenance logs maintained
- ☐ Staff training records kept (3 years minimum)
- ☐ Audit trails enabled and backed up (90 days minimum)
- ☐ Incident reports documented
- ☐ Vendor contracts and SLAs filed

Compliance Verification & Sign-Off

I certify that all applicable compliance requirements have been reviewed:

Compliance Officer: _____ Date: _____

Signature: _____

Legal Counsel: _____ Date: _____

Signature: _____

Next Compliance Review Due: _____ (Recommended: Annual)

Compliance Resources

- ADA Standards: www.ada.gov/2010ADASTandards_index.htm
- NFPA Codes: www.nfpa.org/codes-and-standards
- GDPR Official Text: gdpr-info.eu
- PCI DSS: www.pcisecuritystandards.org
- ICC Building Codes: www.iccsafe.org
- ANSI/BHMA: www.bhma.org