Curotec

✅ Laravel Cloud Compliance Checklist

🔐 Data Security

- ☐ Encrypt data at rest (e.g., AWS KMS), in transit (HTTPS)
- ☐ Use Laravel's Crypt helper for app-level encryption
- ☐ Hash passwords using bcrypt or Argon2
- ☐ Avoid storing sensitive data in logs

👤 User Privacy (GDPR, CCPA, HIPAA)

- ☐ Allow users to view/update/delete personal data
- ☐ Provide privacy policy and obtain user consent
- ☐ Define data retention and anonymization policies
- ☐ Handle tracking data per privacy laws

🛡️ Access Control

- ☐ Use secure Laravel auth (Breeze, Jetstream, Sanctum)
- ☐ Implement RBAC and MFA for admins
- ☐ Use token/session auth for APIs
- ☐ Restrict SSH/cloud console access

🧾 Logging & Monitoring

- ☐ Log user activity, logins, and permission changes
- ☐ Store logs securely and review them regularly
- ☐ Integrate with monitoring tools (e.g., CloudWatch)

🧪 Testing, CI/CD, and Secure Development

- ☐ Run security tests in CI pipeline
- ☐ Never commit secrets to version control
- ☐ Vet and update packages regularly
- ☐ Follow secure SDLC practices

💽 Backup & Disaster Recovery

- ☐ Schedule and encrypt regular backups
- ☐ Test restore procedures quarterly
- ☐ Ensure idempotent queue/scheduler jobs

📄 Compliance Documentation & Policies

- ☐ Maintain DPAs and processing records
- ☐ Define and test incident response plan
- ☐ Assign a DPO or privacy lead
- ☐ Train staff on compliance/security