HMRC API Compliance & Data Protection Guide

Tech Stack Context: TypeScript (client-side), Vite, Firebase

Objective: Ensure full compliance with HMRC API requirements, UK GDPR, and security best practices.

---

1. HMRC Developer Hub Application

Action Items: - Only **1 production application** is needed. Name it after your company. - Do **not create multiple applications** for each customer; use **OAuth tokens** to isolate traffic. - Avoid tight coupling with HMRC APIs; use loose coupling to reduce breakage risk. - Do not import HMRC-specific certificates into keystores; use global root CA keystore. - IP addresses are not static; configure proxy for full domain access instead of firewall rules. - HMRC APIs **do not support CORS**; use Firebase functions as a proxy.

Reference: HMRC Development Practices

---

2. OAuth & API Authorization

Action Items: - Implement OAuth 2.0 on server-side via Firebase functions. - **Do not store credentials client-side.** - Tokens must be encrypted at rest and in transit.

Reference: User Restricted Endpoints

---

3. Data Security & Encryption

Action Items: - Encrypt sensitive data in Firebase (Firestore, Storage). - Use **TLS 1.3** for all network communication. - Secure encryption key management (do not store keys alongside data). - Train developers on encryption use.

Residual Risks: - Metadata exposure (IP, DNS queries). - Access if encrypted device left unlocked.

Reference: ICO Encryption Guidance

---

4. Lawful Basis for Data Processing

Action Items: - Determine lawful basis (Consent, Contract, Legal Obligation, Vital Interests, Public Task, Legitimate Interests). - Document lawful basis before processing. - Include lawful basis in privacy notices. - For **special category or criminal offence data**, identify additional conditions.

Reference: ICO Lawful Basis Guide

---

5. Personal Data Breaches

Action Items: - Prepare breach response plan; assign responsibilities. - Document all breaches. - Notify ICO within 72 hours for notifiable breaches. - Notify affected individuals promptly if high risk. - Preventive measures: training, root cause analysis, audit logs, access controls.

Reference: ICO Personal Data Breaches Guide

---

6. Development & Testing Practices

Action Items: - Follow HMRC DevOps practices: CI/CD, continuous testing. - Automated tests run weekly in sandbox. - Monitor for breaking changes; HMRC gives 6 months notice. - Perform periodic penetration testing. - Follow accessibility standards (WCAG 2.1 AA).

References: - HMRC Testing Guidance - NCSC Penetration Testing

---

7. Service Management & Security

Action Items: - Security incident reporting channel for customers. - Notify HMRC of breaches within 72 hours. - Implement RBAC in Firebase. - Follow NCSC Cloud Security Principles: personnel security, customer separation. - Strong password policies and MFA where possible.

References: - Personnel Security - Customer Separation - Password Guidance

---

8. Marketing & Customer Data

Action Items: - Do **not use HMRC logos** unless allowed. - Marketing must comply with UK law. - Obtain explicit consent before sharing customer data. - Avoid implying HMRC approval.

Reference: HMRC Terms of Use

---

9. Firebase + Vite Considerations

- Do not make client-side API calls to HMRC directly; use Firebase backend.
- Store secrets in Firebase environment variables.
- Run automated CI/CD tests against sandbox.
- Log anonymized events to avoid storing PII unnecessarily.

✅Compliance Checklist

1. [ ] Single production app registered with HMRC Developer Hub.
2. [ ] OAuth implemented server-side; no client-side credentials.
3. [ ] Encryption for data in transit and at rest.
4. [ ] Lawful basis determined and documented.
5. [ ] Breach detection and response plan in place.
6. [ ] Development practices follow HMRC guidance; CI/CD automated testing.
7. [ ] RBAC and access controls in Firebase.
8. [ ] Marketing materials comply with law; consent obtained.
9. [ ] Penetration testing and audits conducted periodically.
10. [ ] Documentation maintained for accountability and compliance.

All links retained for reference and staff guidance.