Mobile Application Data Privacy Risk Checklist

1. Data Collection

- [ ] List all personal data collected by the app.

- [ ] Specify the purpose for each type of data collected.

- [ ] Minimize data collection to only what is necessary.

2. User Consent

- [ ] Obtain explicit user consent before data collection.

- [ ] Provide users with clear privacy policies.

- [ ] Allow users to withdraw consent easily.

3. Data Storage & Security

- [ ] Store all user data securely (e.g., encryption).

- [ ] Limit data access to authorized personnel/app components only.

- [ ] Implement secure data transmission (e.g., HTTPS).

4. Third-party Sharing

- [ ] Disclose all third-party data sharing practices.

- [ ] Review and document all third-party SDKs and privacy policies.

- [ ] Obtain user consent for third-party data sharing.

5. User Rights

☐ Provide mechanisms for users to access, modify, or delete their data.

☐ Allow users to export their data when requested.

☐ Inform users about their privacy rights.

---

6. Compliance & Review

☐ Ensure app compliance with relevant regulations (e.g., GDPR, CCPA).

☐ Regularly review and update app privacy practices.

☐ Document any privacy risks and mitigations identified.