Privacy Audit Review Checklist (1.0)

Before start of review

Sign-In

Review scope has provided:
- System Description
- Audit Scope
- Security Status
- R&D Team Contacts
- Buisness Owner

- **Does the system collect:**
- Personal Details and/or identifiers? (PII)
- Location or Geographical Data? (PII)
- Financial Data? (PCI, SOX)
- Health data? (HIPAA)
- Child related information? (COPPA)
- Communication or social information?
- User-generated content?
- Usernames, Passwords or Authentication Tokens?

- **Is the system deployed**
- In-house vs In-cloud?
- Geographical areas? (eg: China)
- Utilises 3rd parties?

- **Data purpose & usage**
- Primary, Secondary
- 3rd party usage
- Marketing, Advertising
- Profiling
- Caching, Temporary Storage of Data

- **Cross-check previous audits (if made)**

At checkpoints during formal review

Time-Out

- **Confirm all review team members have introduced themselves by name and role**

- **All team members state:**
- Anticipated Events Listed
- Documentation Available

- **Data classification :**
- Security, Information, Provenance, Usage, Purpose
- Data retention & deletion
- Encryption requirements

- **Data Flow:**
- Sources, inputs and output flows.
- Logical and physical data locations
- Iinfrastructure and protocols
- Channel & content security & encryption

- **Legal:**
- Notice, Consents, Terms, Conditions, Policies
- Data Access (Internal & legal authority)

- **UX/UI:**
- Display and update of relevant policies
- Consent mechanisms

- **Procedural and Human Factors**
- Access Control & Partitionig
- Back-office procedures

Before customer report

Sign-Out

- **Confirm review contents, results and recommendations**

- **All team members to confirm:**
- All information shared within the review team

- Data classification performed
- Data flow performed
- Legal review performed
- UX review performed

- Key recommendations made and communicated
- Specific risks recorded and communicated
- Follow-up schedule agreed and communicated
- Data destruction timings and procedures communicated

- Results and review documentation archived

- **Internally review audit process, outcome and suggest improvements if necessary**

This checklist is not intended to be comprehensive. Additions and modification to fit local practice and context are encouraged

Privacy Audit Review Checklist (1.0 Simplified)

Before start of review

Sign-In

Review scope has provided:

- System Description
- Audit Scope
- Security Status
- R&D Team Contacts
- Buisness Owner

- List the collected data
- Describe deployment
- Decribe data purpose and usage
- Cross-check previous audits (if made)

At checkpoints during formal review

Time-Out

- Confirm all review team members have introduced themselves by name and role

- Ensure all documentation is available to all audit team members as necessary

- Data classification performed
- Data Flow modelling performed
- Legal checks and compliances performed
- UX/UI review performed
- Procedural and Human Factors reviewed and documented

Before customer report

Sign-Out

- Confirm review contents, results and recommendations
- All review data shared with audit team
- Key recommendations made
- Specific risks recorded
- Follow-up schedule agreed
- Data destruction timings and procedures
- Results and review documentation archived
- All of the above communicated to all parties as necessary

- Internally review audit process, outcome and suggest improvements if necessary

This checklist is not intended to be comprehensive. Additions and modification to fit local practice and context are encouraged