Final Whistle Card Collection

Data Protection Impact Assessment — Public Summary

Assessment updated: 1 November 2026 | Contact: lennonarthurclarke09@outlook.com

Status and scope

The DPIA covers account and collection data, age and parental-control information, AI scanner requests, subscription-related identifiers, and supporting security and privacy records. This public summary is not legal advice, a certification of compliance, or independent assurance.

Processing covered

Accounts and sign-in: Firebase Authentication is used to create and secure accounts.

Collection management: the application and Firestore store card collection and duplicate records.

Age and parental safeguards: the application and Firestore manage age bands, parent-link and approval state, and feature permissions.

AI card scanning: requests are sent through a Netlify function to OpenAI for card identification; provider-side retention must be distinguished from application storage.

Subscriptions: the application backend and Stripe manage subscription state and payment identifiers; payment-card handling is by Stripe.

Security and support: relevant technical logs, support records, and terms evidence support security, accountability, and support.

Children’s safeguards and observed evidence

The product design blocks under-13 registration and holds ages 13–16 pending email verification and parent confirmation, with feature permissions separately controlled. On 1 November 2026, the operator reported that an under-13 registration attempt was refused and no Firebase record was created. A screenshot showed the 13–16 account waiting for email verification and parent confirmation, with features shown as disabled. These are operator-reported observations; server-side enforcement was not independently verified.

Main risks considered

- Children may misstate age or bypass restrictions; self-declared age has inherent limits.
- Parent approval, permission withdrawal, or account isolation may not be consistently enforced across protected actions.
- Collection or child-safety information could be exposed through misconfigured access rules or privileged functions.
- Scanner requests, logs, or provider records may be retained longer than explained; AI usage may cause unexpected cost or abuse.
- Subscription access, account deletion, privacy requests, breach response, provider terms, and international transfers require accurate implementation and evidence.

Mitigations and remaining conditions

The assessment records age and parental controls, access rules, privileged-function checks, privacy-request and breach procedures, and provider-transfer documentation. Open conditions include verifying server-side child-safety and cross-account controls, scanner and checkout restrictions, deployed retention and deletion, provider settings, privacy-request and incident readiness, and the Children’s Code consultation or a reasoned decision not to consult. Do not treat any unverified control as passed.

Retention note

An expiry timestamp alone does not delete a record. Scheduled cleanup, actual deletion, Firestore configuration, and provider-side retention must be verified before specific deletion periods are promised.

Operator decision and limitations

Decision recorded 1 November 2026: AS READY AS WE CAN GET IT, subject to the pre-launch conditions and feature limits in the DPIA Risk Review and Decision Record. Operator: **LENNON ARTHUR CLARKE**. This decision does not mean all controls have been independently tested or that unresolved risks are closed.

The full internal DPIA and operational records are maintained separately. If a high residual risk cannot be mitigated, the need for prior ICO consultation must be assessed before the affected processing begins. Questions: lennonarthurclarke09@outlook.com.