Legitimate Interests Assessment (LIA)

Project: Tapper Traffic Quality & Ad Fraud Prevention Pilot

Date: _____

Controller: Client / relevant entity (as applicable)

Processor: Tapper AI Ltd (Tapper)

Processing purpose: Fraud prevention, campaign security, and traffic quality measurement for paid media landing traffic.

1) Legitimate interest being pursued

The legitimate interest is to protect the Controller's advertising budgets, digital properties, and campaign integrity by:

- detecting and mitigating invalid or abusive traffic (e.g., bots, automation, click flooding / repeat clicking patterns, suspicious traffic sources), and
- improving the integrity of performance measurement by distinguishing legitimate vs non-legitimate traffic patterns.

This supports:

- preventing waste and misuse of advertising spend,
- reducing exposure to malicious activity that can degrade systems and campaign performance,
- improving the reliability of optimisation and performance decisions.

2) Necessity test

Why the processing is necessary

Invalid or fraudulent traffic often mimics legitimate user behaviour and cannot be reliably identified using ad platform reporting alone. The processing is necessary to:

- observe landing behaviour around the time of the click,
- identify patterns indicative of invalid traffic or abuse (e.g., high-frequency repeat clicks in short windows, anomalous session progression),
- support mitigation actions (e.g., exclusions / blocking at the ad platform level where enabled).

Why less intrusive means are insufficient

Alternative measures (manual reviews, basic IP filters, or platform-only signals) are typically insufficient because:

- invalid traffic tactics evolve quickly and are distributed across devices and networks,
- platform data is not always granular enough to detect abusive landing behaviour,
- manual approaches are slow, inconsistent, and do not scale to real-time fraud patterns.

3) Balancing test

Nature of the data processed (data minimisation)

Tapper's processing is limited to what is required to analyse traffic quality and detect abuse. Typical data categories include:

- online identifiers (e.g., IP address, user agent, cookie / device identifiers where configured and permitted),
- session and event metadata (timestamps, page / path, basic interaction and session progression signals),
- ad click context and campaign metadata (e.g., URL parameters / click IDs such as gclid / fbclid and platform campaign or ad identifiers where available),
- operational and security logs needed for troubleshooting and auditability.

Special category data: Not processed (not applicable).

Intent: The processing focuses on traffic patterns and fraud signals, not on identifying individuals as real-world persons.

Reasonable expectations of individuals

Users who click ads and visit a commercial website can reasonably expect:

- standard security and anti-abuse protections,
- measures to prevent malicious activity and protect service integrity,
- processing necessary to ensure advertising and site operations are not abused.

Impact on individuals

Potential impacts are assessed as low to moderate, depending on configuration:

- data relates primarily to online identifiers and session signals, not sensitive data,
- consequences are limited to traffic being classified as invalid and, where enabled, excluded from future ad exposure or landings for campaign protection.

Measures to ensure fairness and reduce impact

Safeguards include:

- purpose limitation (fraud prevention / campaign security only),
- data minimisation and restricted access,
- configurable thresholds and review to reduce false positives,
- appropriate transparency via the Controller's privacy and cookie disclosures.

Device identifiers and purpose limitation (PECR context)

Tapper is used for fraud prevention and security. Any access to device identifiers is limited to what is necessary to detect and mitigate invalid traffic and protect campaign integrity, and is not used for advertising or marketing profiling. The Controller should align CMP categorisation and user-facing disclosures accordingly. If the Controller's PECR policy requires opt-in consent for device identifier access, Tapper can be configured to activate only after consent is obtained.

4) Retention

Retention period: Personal data (pseudonymous logs, online identifiers, and related event records) is retained for up to 12 months (365 days), unless a shorter period is agreed in writing for the pilot or retention is required by applicable law or contractual obligation.

Retention supports investigation of repeat abuse patterns, trend analysis, and auditability during and after the pilot period.

5) Safeguards and controls

Tapper applies safeguards appropriate for the risk profile, including:

- encryption in transit (TLS 1.2+) and encryption at rest,
- least-privilege access controls, RBAC, and MFA for privileged access,
- logging and monitoring for security and audit purposes,
- sub-processor governance (documented sub-processors and contractual controls),
- incident management and breach notification commitments per the DPA and security documentation,
- client-side redaction controls to avoid capturing form field contents where feasible and configured.

6) International transfers

Where personal data is transferred across borders (including hosting or processing in the EEA or transfers outside the UK / EEA), transfers are protected using the applicable mechanism set out in the DPA or transfer documentation (e.g., UK IDTA and / or EU SCCs as applicable), plus supplementary measures where required.

7) Relationship to PECR / cookie consent

This LIA addresses the GDPR lawful basis (Legitimate Interests) for processing personal data for fraud prevention and campaign security.

Where Tapper accesses device identifiers (cookies or device IDs), the Controller should ensure this is handled in line with PECR and cookie consent requirements through CMP / GTM configuration and appropriate disclosures (assessed separately from the GDPR lawful basis).

8) Conclusion

Based on the necessity and balancing tests, the Controller's legitimate interests in fraud prevention and campaign security are not overridden by individuals' rights and freedoms, provided the safeguards, minimisation, retention limits, and transparency measures described above are applied.

Outcome: Legitimate Interests is an appropriate GDPR lawful basis for this processing for fraud prevention and campaign security (subject to Controller approval and PECR consent measures where device identifiers are accessed).

9) Approval

Controller reviewer: _____

Title: _____

Date: _____

Controller approval: ☐ Approved ☐ Approved with conditions ☐ Not approved

Notes / conditions: _____

Processor acknowledgement (Tapper): _____

Title: _____

Date: _____