

PRIVACY POLICY

M360 SOLUTIONS GROUP LIMITED

Effective Date: 1st November, 2026.

Version: 001

1. PREAMBLE AND REGULATORY FRAMEWORK

M360 Solutions Group Limited ("M360", "we", "us", or "our") is committed to processing personal data lawfully, fairly, transparently, and securely.

This Privacy Policy governs the processing of personal data in connection with M360's white label advertising technology platform hereinafter refers as **(the "Platform")**. The Platform is powered by technology proprietary to Eskimi **("Eskimi")** and made available to clients and partner agencies under the M360 brand.

This Policy is issued in accordance with the Constitution of the Federal Republic of Nigeria, 1999 (as amended), particularly Section 37; The Nigeria Data Protection Act, 2023 ("NDPA"); The Nigeria Data Protection Act General Application and Implementation Directive, 2025 ("GAID"); All regulations, guidance notices, directives, and orders issued by the Nigeria Data Protection Commission ("NDPC"); and Other applicable Nigerian laws and regulations. Together, these are referred to as the "Applicable Data Protection Laws."

2. SCOPE

This Policy applies to:

Clients: Advertisers and other entities for whom M360 executes advertising campaigns through the Platform;

Partner Agencies: Third party agencies granted access to the Platform through M360 to provide advertising services to their own clients;

End Users: Natural persons whose personal data is processed in connection with advertising campaigns delivered through the Platform;

Representatives: Directors, officers, employees, agents, and contact persons of Clients and Partner Agencies;

Website visitors and Platform users: Individuals who access M360's website, dashboards, reporting tools, or support channels; and

Prospective clients, vendors, and business partners: Individuals whose personal data is collected during commercial engagement with M360.

3. POLICY HIERARCHY

This Policy forms part of M360's data protection governance framework. Where a written Data Processing Agreement **("DPA")**, Joint Controller Arrangement, campaign terms, client agreement, or agency agreement contains more specific data protection obligations, those terms shall prevail over this Policy to the extent of any inconsistency. Nothing in this Policy limits or excludes any right available to a Data Subject under the NDPA or GAID.

4. DEFINITIONS AND INTERPRETATION

In this Policy, unless the context otherwise requires:

- a. **"Data Controller"** means a person or entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.
- b. **"Data Processor"** means a person or entity that processes personal data on behalf of, and on the documented instructions of, a Data Controller.
- c. **"Data Subject"** means an identified or identifiable natural person to whom personal data relates.
- d. **"Joint Controllers"** means two or more entities that jointly determine the purposes and means of a processing activity.
- e. **"Personal Data"** means any information relating to an identified or identifiable natural person, including pseudonymized data capable of reidentification.
- f. **"Sensitive Personal Data"** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, sexual orientation, or other categories prescribed under applicable law.
- g. **"Processing"** means any operation performed on personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, transmission, dissemination, restriction, erasure, or destruction.
- h. **"Sub-Processor"** means a third party engaged by M360 or a Data Processor to process personal data on behalf of a Data Controller.
- i. **"Consent"** means a freely given, specific, informed, and unambiguous indication of a Data Subject's agreement to the processing of personal data.
- j. **"Data Privacy Impact Assessment" or "DPIA"** means an assessment conducted to identify and minimize data protection risks arising from processing activities likely to result in a high risk to the rights and freedoms of Data Subjects.
- k. **"SNAG"** means a Data Subject's Standard Notice to Address Grievance issued under the GAID.
- l. Words importing the singular include the plural and vice versa. Headings are for convenience only and do not affect interpretation.

5. DATA CONTROLLER AND PROCESSOR ROLES IN THE WHITE LABEL ARRANGEMENT

5.1 White Label Structure:

M360 operates the Platform as a white label solution. Eskimi's advertising technology is presented and made commercially available under the M360 brand.

M360 maintains a parent account through which it provides and administers sub accounts for Clients and Partner Agencies. Clients and Partner Agencies access Eskimi's advertising services through M360, while M360 retains administrative oversight of their accounts and campaigns.

5.2 Allocation of Roles:

The classification of M360, Clients, Partner Agencies, and Eskimi as Data Controllers, Data Processors, or Joint Controllers depends on the actual processing activity and the degree of control exercised over the purposes and means of processing, rather than contractual labels alone.

(a) M360 as Data Controller:

M360 acts as a Data Controller in respect of the establishment, administration, security, and oversight of the parent account and sub accounts.

The management of its commercial relationships with Clients, Partner Agencies, Eskimi, vendors, and prospective business partners.

The processing of registration, account, billing, communication, and support data relating to Client and Partner Agency representatives.

Campaign execution where M360 determines or materially influences the campaign objective, audience selection, targeting parameters, creative deployment, optimization strategy, or measurement methodology;

Compliance with M360's own legal, tax, regulatory, and corporate obligations; and the operation, improvement, and protection of the Platform.

(b) M360 as Data Processor:

M360 acts as a Data Processor where it processes End User personal data solely on the documented instructions of a Client or Partner Agency for the purpose of executing an advertising campaign, and where M360 does not determine the purposes or essential means of that processing.

In such circumstances, the Client or Partner Agency remains responsible for ensuring that it has a lawful basis for the processing, that appropriate notices and consents have been obtained where required, and that the personal data supplied to M360 is accurate, lawful, and permitted for the intended use.

(c) Joint Controlership:

M360 and a Client or Partner Agency may act as Joint Controllers where they jointly determine the purposes and means of a particular processing activity, including

collaborative decisions relating to campaign targeting, audience segmentation, measurement, or data enrichment.

Where Joint Controllorship applies, the parties shall document their respective responsibilities in a Joint Controller Arrangement or applicable campaign terms, including responsibility for providing privacy information to Data Subjects; Responding to Data subject requests; handling complaints and SNAG notices; securing personal data; notifying the NDPC and affected Data subjects of personal data breaches; and allocating liability between the parties.

(d) Eskimi's Role

Eskimi acts as a Sub Processor to M360 in respect of personal data processed through the Platform technology on M360's documented instructions.

Eskimi shall process such personal data only in accordance with a written sub processing agreement imposing data protection obligations no less protective than those applicable to M360 under the NDPA, GAID, and this Policy. Where Eskimi independently determines the purposes or means of processing, including for platform level analytics, fraud prevention, security, product improvement, or compliance with its own legal obligations, Eskimi may act as an independent Data Controller or Joint Controller. In such cases, Eskimi's own privacy notice and applicable agreements shall govern that processing to the extent disclosed to M360 and permitted under the commercial arrangement.

(e) Partner Agencies

A Partner Agency acts as: A Data Controller where it determines the purposes and means of processing personal data for its own business or its own clients; and A Data Processor where it processes personal data solely on behalf of its own clients.

M360 does not control the independent processing activities of Partner Agencies and is not responsible for their compliance with Applicable Data Protection Laws. As a condition of access to the Platform, each Partner Agency shall:

- a.** Maintain a lawful basis for processing personal data;
- b.** Provide compliant privacy notices to its clients and End Users where required;
- c.** Obtain all necessary consents and permissions;
- d.** Ensure that audience lists and campaign data are lawfully sourced;
- e.** Comply with the NDPA, GAID, and applicable advertising regulations;
- f.** Not upload, target, or process Sensitive Personal Data without M360's prior written approval; and
- g.** Indemnify M360 against losses, claims, penalties, and liabilities arising from the Partner Agency's unlawful or unauthorised processing.

6. DATA PROTECTION PRINCIPLES

M360 processes personal data in accordance with the following principles:

- a. **Lawfulness, fairness, and transparency:** Personal data is processed only on a valid legal basis and in a manner transparent to Data Subjects.
- b. **Purpose limitation:** Personal data is collected for specified, explicit, and legitimate purposes and is not further processed incompatibly with those purposes.
- c. **Data minimization:** M360 collects only personal data that is adequate, relevant, and limited to what is necessary.
- d. **Accuracy:** Reasonable steps are taken to ensure personal data is accurate, complete, and kept up to date.
- e. **Storage limitation:** Personal data is retained only for as long as necessary.
- f. **Integrity and confidentiality:** Appropriate technical and organizational safeguards protect personal data.
- g. **Accountability:** M360 maintains records, policies, assessments, and controls to demonstrate compliance with Applicable Data Protection Laws.

7. CATEGORIES OF PERSONAL DATA COLLECTED

7.1 Account and Commercial Data

a. M360 may collect and process:

Identity and contact data, including name, company name, job title, email address, telephone number, and business address, account credentials, authentication data, user roles, and access permissions, billing, invoicing, payment, and transaction data; commercial communications, proposals, contracts, instructions, campaign briefs, and support records; KYC, onboarding, tax, and regulatory information where required.

b. Campaign and Platform Data

In connection with advertising campaigns, M360 or Eskimi may process:

Device and technical data, including IP address, device identifiers, browser type and version, operating system, language settings, and network information, advertising interaction data, including impressions, clicks, views, conversions, engagement events, and campaign performance metrics, audience and targeting data, including inferred or supplied demographic segments, interest categories, behavioral signals, and location data where enabled and lawful; Cookie, pixel, SDK, mobile advertising identifier, and other tracking data; Fraud prevention, security, and abuse detection data.

7.2 Website and Support Data

a. M360 may collect:

Website usage data, including pages visited, links clicked, session duration, and referral sources; login and audit logs; support enquiries, complaints, and correspondence.

7.3 Sensitive Personal Data

M360 does not intentionally collect or process Sensitive Personal Data through the Platform. Clients and Partner Agencies are prohibited from configuring campaigns or uploading audience data involving Sensitive Personal Data without M360's prior written consent and the implementation of enhanced safeguards required under the NDPA and GAID.

Where Sensitive Personal Data is knowingly or inadvertently received, M360 may restrict access, suspend the relevant campaign or account, delete the data where appropriate, and require the Client or Partner Agency to provide written confirmation of the lawful basis for processing.

8. LAWFUL BASES FOR PROCESSING

M360 processes personal data only where one or more lawful bases apply under the NDPA and GAID.

8.1 Contractual Necessity

Processing is necessary for the performance of a contract with a Client, Partner Agency, vendor, or other business partner, including Platform access, campaign execution, reporting, invoicing, and customer support.

8.2 Legitimate Interests

Processing is necessary for M360's legitimate interests, provided such interests are not overridden by the rights and freedoms of Data Subjects. These interests include:

- a.** Administration and security of the Platform;
- b.** Fraud detection, prevention, and investigation;
- c.** Service improvement and product development;
- d.** Business continuity and risk management;
- e.** Enforcement of contractual rights and defence of legal claims;
- f.** Business to business communications concerning services relevant to the recipient's professional role.
- g.** Where M360 relies on legitimate interests, it conducts and documents a Legitimate Interest Assessment ("LIA").

8.3 Consent

Where consent is required, including for non essential cookies, tracking technologies, direct marketing, or certain audience targeting activities, M360 ensures that consent is freely given, informed, and unambiguous.

Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.

8.4 Legal Obligation

Processing may be necessary to comply with legal or regulatory obligations, including tax, accounting, anti money laundering, consumer protection, advertising, and data protection requirements.

8.5 Vital Interests and Public Interest

M360 may process personal data where necessary to protect the vital interests of a Data subject or another person, or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, where applicable.

9. PURPOSES OF PROCESSING

M360 processes personal data for the following purposes:

- a. Platform Administration:** creating and managing the parent account, provisioning and administering sub accounts, managing user access, and maintaining Platform security.
- b. Campaign Execution:** configuring, launching, delivering, targeting, optimizing, and measuring advertising campaigns.
- c. Reporting and Analytics:** generating performance reports, providing campaign insights, and conducting Platform-level analytics.
- d. Billing and Financial Management:** processing payments, issuing invoices, reconciling accounts, and maintaining financial records.
- e. Customer Support:** responding to enquiries, resolving technical issues, and managing complaints.
- f. Compliance and Risk Management:** complying with legal obligations, responding to lawful requests, preventing fraud, and protecting M360's rights and safety.
- g. Service Communications:** sending administrative, operational, security, and service related communications.
- h. Business Development:** communicating with existing and prospective Clients and Partner Agencies about relevant services, subject to applicable consent and opt-out rights.
- i. Security and Fraud Prevention:** detecting unauthorised access, suspicious activity, invalid traffic, and abuse of the Platform.

M360 will not use personal data for purposes that are incompatible with the original purposes without a valid lawful basis and, where required, appropriate notice or consent.

10. DATA SHARING AND DISCLOSURE

10.1 Sharing with Eskimi

- a.** M360 shares personal data with Eskimi only to the extent necessary for the operation of the Platform and the delivery of advertising services.
- b.** Eskimi processes such data as a Sub Processor in accordance with the applicable sub processing agreement.
- c.** Eskimi shall not use personal data received from M360 for its own independent purposes except as expressly permitted under the agreement, permitted by law, or disclosed in Eskimi's own privacy documentation where Eskimi acts as an independent Controller.

10.2 Sharing with Clients and Partner Agencies

- a.** M360 makes available to Clients and Partner Agencies the campaign data and reporting necessary for them to assess the performance of their advertising activities.
- b.** Where a client or partner agency is a Data Controller or Joint Controller, its subsequent processing of that data is governed by its own privacy notice and legal obligations.
- c.** M360 does not authorize any Client or Partner Agency to use data received through the Platform for incompatible purposes.

10.3 Sharing with Service Providers

- a.** M360 may engage third party service providers, including cloud hosting providers, payment processors, analytics providers, cybersecurity providers, communication tools, and customer support platforms.
- b.** Such providers are engaged under written agreements imposing confidentiality, security, data protection, and sub processing obligations consistent with the NDPA and GAID.
- c.** A current list of material Sub Processors is available upon written request to the Data Protection Officer.

10.4 Advertising and Technology Partners

- a.** Where necessary for campaign delivery, measurement, frequency capping, fraud prevention, or performance reporting, personal data may be shared with advertising exchanges, publishers, demand side or supply side platforms, measurement providers, and data providers.
- b.** Such sharing occurs only where permitted by law, supported by appropriate contractual safeguards, and subject to applicable consent, opt-out, or transparency requirements.

10.5 Legal and Regulatory Disclosures

- a. M360 may disclose personal data where required by law, regulation, court order, or a lawful request from a competent authority, including the NDPC.
- b. Where legally permissible, M360 will notify the affected Data Subject of the disclosure. Where disclosure is prohibited by law, M360 may be unable to provide such notice.

10.6 Corporate Transactions

- a. In connection with a merger, acquisition, restructuring, financing, sale of assets, or similar corporate transaction, personal data may be transferred to a successor entity or prospective transaction party.
- b. Any such transfer shall be subject to confidentiality obligations and data protection safeguards no less protective than those in this Policy.

10.7 No Sale of Personal Data

M360 does not sell personal data. M360 does not disclose personal data to third parties for their independent direct marketing purposes without a valid lawful basis and, where required, the Data Subject's consent.

11. INTERNATIONAL DATA TRANSFERS

Personal data processed through the Platform may be transferred to, stored in, or accessed from jurisdictions outside Nigeria, including where Eskimi, its affiliates, cloud providers, or other Sub Processors are located.

12. COOKIES AND TRACKING TECHNOLOGIES

The Platform and M360 websites use cookies, pixels, tags, SDKs, and similar technologies to:

- a. Enable core functionality;
- b. Maintain secure sessions;
- c. Remember user preferences;
- d. Measure website and campaign performance;
- e. Support advertising delivery, frequency capping, and audience measurement;
- f. Detect fraud and improve security.
- g. Non-essential cookies and tracking technologies are deployed only after valid consent has been obtained where required.
- h. M360's consent management mechanism is designed to:
 - i. Present clear information about cookie categories and purposes;
 - j. Obtain affirmative consent before non-essential cookies are set;

- k.** Record consent preferences;
- l.** Enable withdrawal of consent with equal ease;
- m.** Respect recognised opt out signals and browser-based privacy controls where technically feasible.

Data Subjects may manage cookies through their browser or device settings. Disabling certain cookies may limit Platform functionality or affect campaign performance.

13. DIRECT MARKETING AND OPT OUTS

- a.** M360 may send marketing communications to business contacts and prospective Clients or Partner Agencies where permitted by law.
- b.** Every marketing communication shall include a clear and accessible opt out mechanism. Data Subjects may object to direct marketing at any time by:
 - c.** Clicking the unsubscribe link in the communication;
 - d.** Contacting the Data Protection Officer; or
 - e.** Updating communication preferences through the Platform, where available.
- f.** Upon receipt of a valid opt out request, M360 shall cease marketing communications to that Data Subject without undue delay.

This Section does not apply to essential service, security, billing, legal, or administrative communications.

14. CHILDREN'S DATA

The Platform and M360's advertising services are not directed to children.

- a.** M360 does not knowingly collect personal data from children without the consent of a parent or legal guardian where such consent is required under applicable law.
- b.** Clients and Partner Agencies must not target children or upload children's personal data through the Platform without M360's prior written approval and compliance with all applicable legal requirements.
- c.** If M360 becomes aware that it has collected a child's personal data without appropriate consent, it will take reasonable steps to delete the data and suspend any related processing.

15.AUTOMATED DECISION MAKING AND PROFILING

The Platform may use automated processes, algorithms, machine learning tools, and profiling techniques to support advertising delivery, audience segmentation, bid optimization, conversion measurement, fraud detection, and campaign performance analysis.

Such processing may involve automated decisions regarding the advertisements shown to End Users, the frequency of exposure, or the audience categories to which an advertisement is delivered.

Where automated decision making produces legal effects or similarly significantly affects a Data Subject, M360 will implement appropriate safeguards, including:

- a.** Meaningful information about the logic involved;
- b.** Information on the significance and envisaged consequences of the processing;
- c.** The right to obtain human intervention where applicable;
- d.** The right to express a point of view;
- e.** The right to contest the decision; and
- f.** The right to object to profiling for direct marketing.

Where required by the NDPA or GAID, M360 shall conduct a DPIA before commencing high risk profiling or automated decision making activities.

16.DATA RETENTION

M360 retains personal data only for as long as necessary to fulfil the purposes for which it was collected or as required by law. Retention periods are determined by reference to:

- a.** The duration of the contractual relationship with the relevant Client or Partner Agency;
- b.** The duration of the advertising campaign and any post-campaign reporting or reconciliation period;
- c.** Statutory retention obligations relating to financial, tax, accounting, employment, and corporate records;
- d.** Limitation periods for potential legal claims;
- e.** Security, fraud prevention, and dispute-resolution requirements; and
- f.** Operational requirements of the Platform.

- g.** Upon expiry of the applicable retention period, personal data shall be securely deleted or irreversibly anonymized.
Where immediate deletion is technically impracticable, including data contained in backup archives, M360 shall isolate and protect the data, prevent further processing, and delete it once deletion becomes practicable.

17. DATA SECURITY

M360 implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- a.** Encryption of personal data in transit and, where appropriate, at rest;
- b.** Role based access controls and the principle of least privilege;
- c.** Multi factor authentication for administrative and privileged access;
- d.** Secure configuration of the parent account and sub accounts;
- e.** Audit logging, monitoring, and access review procedures;
- f.** Vulnerability management, penetration testing, and security assessments;
- g.** Network, endpoint, and application security controls;
- h.** Confidentiality obligations imposed on employees and contractors;
- i.** Data protection and information-security training;
- j.** Incident response, disaster recovery, and business continuity plans;
- k.** Vendor due diligence and ongoing Sub Processor oversight.

M360 reviews and updates its security measures regularly in light of technological developments, emerging threats, and regulatory guidance.

18. DATA BREACH NOTIFICATION

In the event of a personal data breach, M360 shall:

- a.** Promptly investigate, contain, and assess the breach;
- b.** Notify the NDPC within 72 hours of becoming aware of a breach likely to result in a risk to the rights and freedoms of Data Subjects;
- c.** Notify affected Data Subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms;

- d.** Where M360 acts as a Data Processor, notify the relevant Data Controller without undue delay and provide reasonable assistance to enable the Controller to meet its legal obligations;
- e.** Maintain a breach register documenting the facts, effects, remedial actions, and notifications made; and
- f.** Cooperate with the NDPC, Data Controllers, and other relevant authorities as required.
- g.** Where it is not possible to provide all information immediately, M360 may provide the information in phases without undue further delay.

19.COMPLAINTS AND SNAG PROCESS

Data Subjects are encouraged to contact M360's Data Protection Officer in the first instance where a Data Subject believes that M360 has violated Applicable Data Protection Laws, the Data Subject may submit a Data Subject's Standard Notice to Address Grievance ("SNAG") in accordance with the GAID.

M360 shall acknowledge and address valid SNAG notices in accordance with the applicable regulatory procedure. A Data Subject retains the right to escalate a complaint directly to the NDPC after officially writing to M360 severally and M360 ignored to attend to them.

20.DATA PROTECTION GOVERNANCE

20.1 Data Protection Officer

M360 has designated a Data Protection Officer ("DPO") to oversee compliance with this Policy and Applicable Data Protection Laws.

The DPO's responsibilities include:

- a.** Advising M360 on its obligations under the NDPA and GAID;
- b.** Monitoring compliance with this Policy and internal procedures;
- c.** Serving as the contact point for Data Subjects, Clients, Partner Agencies, and the NDPC;
- d.** Coordinating Data Subject requests, breach response, and DPIAs;
- e.** Maintaining records of processing activities;
- f.** Providing data protection training and awareness programmes; and
- g.** Reporting to M360 management on data protection risks and compliance.

20.2 Privacy by Design and by Default

- a.** M360 applies privacy by design and by default in the development, procurement, configuration, and operation of the Platform.
- b.** This includes assessing privacy risks before implementing new features, minimizing data collection, limiting access, using pseudonymization or aggregation where appropriate, and embedding security controls into Platform workflows.

20.3 Data Privacy Impact Assessments

M360 shall conduct a DPIA where processing is likely to result in a high risk to the rights and freedoms of Data Subjects, including large scale profiling, systematic monitoring, use of Sensitive Personal Data, or cross border transfers where required.

DPIAs shall assess the necessity, proportionality, risks, and mitigation measures associated with the processing and shall be maintained as part of M360's accountability records.

20.4 Records of Processing Activities

M360 maintains appropriate records of its processing activities, including the purposes of processing, categories of Data Subjects and personal data, recipients, cross-border transfers, retention periods, and security measures.

21. CONTACT DETAILS

Data Protection Officer:
M360 Solutions Group Limited
Omole Phase 1, Lagos Nigeria.
Email: m360solutionslimited@gmail.com

Data Subjects are encouraged to contact M360's DPO in the first instance. Data Subjects also have the right to lodge a complaint directly with the DPO.

22. THIRD PARTY WEBSITES AND SERVICES

- a.** The Platform, M360's website, and campaign materials may contain links to third party websites, applications, or services.
- b.** This Policy does not apply to third party websites or services that are not owned or controlled by M360.
- c.** M360 is not responsible for the privacy practices of third parties.

Data Subjects are encouraged to review the privacy policies of any third party website or service before providing personal data.

23.CHANGES TO THIS PRIVACY POLICY

- a.** M360 may update this Policy from time to time to reflect changes in Applicable Data Protection Laws, regulatory guidance, technology, business arrangements, or processing activities.
- b.** The updated Policy will be published with a revised copy effective date and version number.
- c.** Material changes affecting Clients, Partner Agencies, or Data Subjects will be communicated through the Platform, email, or another appropriate channel.
- d.** Where changes affect processing based on consent, M360 will obtain fresh consent where required.

24.GOVERNING LAW AND DISPUTE RESOLUTION

- a.** This Policy shall be governed by and construed in accordance with the laws of the Federal Republic of Nigeria.
- b.** Any dispute arising out of or in connection with this Policy shall be subject to the exclusive jurisdiction of the courts of Nigeria, without prejudice to:
 - A Data Subject's right to lodge a complaint with the NDPC;
 - Any applicable alternative dispute resolution mechanism; and
 - Any mandatory regulatory process under the NDPA or GAID.

25.SEVERABILITY AND INTERPRETATION

- a.** If any provision of this Policy is held invalid, illegal, or unenforceable, the remaining provisions shall remain in full force and effect.
- b.** The invalid provision shall be modified to the minimum extent necessary to make it valid and enforceable, while preserving the commercial and legal intent of the Policy.

26.POLICY REVIEW

M360 shall review this Policy where required by:

- a.** A change in law or regulatory guidance;
- b.** A material change in the Platform or data flows;
- c.** A new Sub Processor arrangement;
- d.** A personal data breach or security incident;
- e.** A material change in the M360/Eskimi white label arrangement; or
- f.** A direction from the NDPC.

END