APPROVED POLICY DOCUMENT

TORRID PETRIC
LEGACY ENTERPRISES LTD

DATA PROTECTION AND PRIVACY POLICY

Empowering Visions of Brands: Packaging the Future Sustainably

How the Company collects, uses, stores, shares, protects and disposes of personal data processed through the **Torrid Petric Accounting System**.

DOCUMENT REFERENCE	VERSION	STATUS	EFFECTIVE DATE
TP-DPP-001	1.0	APPROVED	8 September 2026

Torrid Petric Legacy Enterprises Ltd • Torrid Petric Accounting System

Approving Authority: Director, **Torrid Petric Legacy Enterprises Ltd**

Version Date: 9 October 2026 · System Code: TP-DPP-001 · Audit Token: ff8dcf953fd238c0…

Contents

1 Introduction

2 Data Controller And Contact

3 Data Sources And Categories Of Personal Data

4 How We Use Your Personal Data

5 Legal Basis For Processing

6 Data Sharing And Disclosure

7 Special Personal Data

8 Microsoft 365 And Third-Party Integrations

9 Social-Media Publishing

10 AI-Assisted Processing

11 Data Retention

12 Data Security

13 Data Subject Rights

14 Cookies And Electronic Communications

15 Personal Data Relating To Children

16 International Data Transfers

17 Aggregated And Anonymised Data

18 Personal Data Breach Notification

19 Changes To This Policy

20 Complaints

21 Approval And Signature

Torrid Petric Legacy Enterprises Ltd

EmpoweringVisionsofBrands:PackagingtheFutureSustainably DATA PROTECTION AND PRIVACY POLICY Document Reference: TP-DPP-001 1.0 Version:

Status: APPROVED Approving Authority: Director, **Torrid Petric Legacy Enterprises Ltd**

1 INTRODUCTION

1.1 **Torrid Petric Legacy Enterprises Ltd** ("the Company", "we", "us", or "our") operates the **Torrid Petric Accounting System** ("the Platform") and may, from time to time, engage in other current or reasonably foreseeable business activities that involve the processing of personal data. This Data Protection and Privacy Policy ("the Policy") sets out how we collect, use, store, share, protect, and dispose of personal data processed by the Company, whether through the Platform or through any other business activity of the Company.

1.2 This Policy is prepared in accordance with the Data Protection and Privacy Act, 2019 (Cap. 97) of Uganda and the Data Protection and Privacy Regulations, 2021. It applies to all personal data processed by the Company in the course of its operations, whether through the Platform or otherwise.

1.3 This Policy forms part of, and is incorporated into, our Terms and Conditions. It should be read alongside our Information and Security Policy, which details the technical and organizational security measures implemented to protect personal data.

This Policy applies to all data subjects whose personal data is processed by the 1.4 Company, including employees, customers and clients, visitors and guests, beneficiaries, volunteers, suppliers, contractors, and any other individuals whose personal data the Company may process in the course of its operations. Specific categories of data subjects include personal account holders, business account owners and members, property module owners and team members, POS module owners and team members, employee portal users, advertisers, Mindcheck participants, newsletter subscribers, job applicants and recruitment candidates, community participants, referees, and visitors.

2 DATA CONTROLLER AND CONTACT

2.1 The Company is the data controller responsible for personal data processed by the Company, whether through the Platform or otherwise.

2.2 Contact details:

Torrid Petric Legacy Enterprises Ltd

Komamboga, Waligo Road, Kampala, Uganda

torridpetriclegacyent.ltd@gmail.com

+256 781860240 A Data Protection Officer (DPO) has been appointed. The DPO's contact details are 2.3 maintained in the Platform's Site Configuration and auto-injected into this policy.

Current DPO: Wanyera Cuthbert Douglas (email: wanye_cuth@yahoo.co.uk, phone: +256 772440377, address: P.O. Box 7051, Kampala Mulago School of Nursing and Midwifery).

3 DATA SOURCES AND CATEGORIES OF PERSONAL DATA

3.1 Data Sources

The Company collects and processes personal data from the following categories of data subjects, whether through the Platform or through any other current or reasonably foreseeable business activity of the Company:

1. Employees: current and prospective employees, including personnel accessed through the employee portal
2. Customers and Clients: personal account holders, business account owners and members, property module owners and team members, POS module owners and team members, advertisers, and any other customers or clients of the Company
3. Visitors and Guests: visitors to the Platform's public pages, blog, and landing site, and visitors to the Company's premises or events
4. Beneficiaries: beneficiaries designated in wills, estate plans, insurance nominations, and any other beneficiary arrangements managed by or through the Company
5. Volunteers: volunteers and voluntary participants in the Company's programmes, including recruitment candidates applying for volunteer roles
6. Suppliers: suppliers of goods and services to the Company
7. independent contractors, consultants, and service providers engaged Contractors: by the Company and

8. Other: any other data subjects whose personal data the Company may reasonably process in the course of its current or foreseeable operations, including newsletter subscribers, community participants, and referees provided by recruitment candidates.

3.2 Identifiers

The Company may collect and process identifiers that directly identify a person or can be used to distinguish them from others, including: first name, last name, nationality, marital status, email address, bank account name, national identification number (e.g.

NIN for Uganda, KRA PIN for Kenya, Ghana Card for Ghana), social security number (e.g.

NSSF number), driver's licence number, date of birth, gender, place of birth, current residence, sector/occupation, account type, and other identifiers assigned by government or financial institutions.

3.3 Individual's Commercial Information

The Company may collect and process information related to an individual's ownership of property, financial transactions, and purchasing behaviour, including: purchasing habits, records of personal property (including assets, land titles, and property records managed through the property module), income, expenses, savings, loans, budgets, will and estate planning data, financial summaries and reports, business names, sector classifications, and other commercial information.

3.4 Sensory Data

The Company may collect and process information captured through sound or visual recordings, including: visual data (profile photos, digital signatures, seals, document attachments, front/back images of national ID cards screened by AI vision for authenticity, blog post media, advertising creative assets, music tracks, interview videos, intro videos, and other images) and audio data (audio recordings transcribed through the Platform's transcription features, where applicable).

3.5 Internet or Similar Network Activity

The Company may collect and process information generated when a person uses websites, applications, or digital services, including: browsing history, search history, Internet Protocol (IP) address, interactions with the Platform's websites, applications, or advertisements, device information, browser type, access times, pages viewed, and usage analytics.

3.6 Geolocation Data

The Company may collect and process geolocation data, including GPS data or other geographical data collected from devices or online activity, when explicitly enabled for document sign-off, application location verification, or other features where location is necessary for the Company's operations.

3.7 Education Information

The Company may collect and process information relating to an individual's academic background, qualifications, certifications, and educational achievements, including: educational qualifications, curriculum vitae (CV), transcripts, certificates, licensure documents, and other educational achievements. This is collected primarily through the recruitment process and may be collected in other contexts as reasonably required.

3.8 Professional or Employment Related Information

The Company may collect and process information connected to a person's work history, professional status, performance records, and participation in professional organisations, including: professional association membership, performance evaluations, disciplinary actions, work experience, leadership experience, referee contact details, employment records, payroll records, attendance records, leave records, daily work reports, and meeting minutes.

3.9 Inferences Drawn from Other Personal Data

The Company may derive inferences from personal data to create individual profiles, including: preferences, behaviour, aptitude, characteristics, attitudes, psychological trends, intelligence, predisposition, and abilities. Such inferences are generated through AI-assisted analysis (including Mindcheck results, financial health assessments, CV screening, and conversion/gamification profiling) and are used only for the purposes for which the underlying data was collected, subject to the safeguards in this Policy. The Company does not make solely automated decisions with significant effects on data subjects without a lawful basis and, where required, the data subject's right to human intervention.

3.10 Special Personal Data

The Company may process special categories of personal data - highly sensitive information that reveals private aspects of an individual's identity, beliefs, health, biology, finances, or personal life - only where processing is necessary, lawful, and accompanied by appropriate safeguards, including explicit consent where required by law. These categories include:

9. Health status or medical records: Mindcheck responses relating to mental and financial wellness, medical checkup forms submitted by recruitment candidates, and any other health data reasonably required for the Company's operations
10. Biometric data: WebAuthn/FIDO2 credential identifiers and public keys used for biometric login and sensitive-action approvals across all account types. Biometric templates are stored locally on the user's device the Company stores only the public key portion. Users may enroll and revoke biometric credentials at any time
11. Financial information: bank account details, mobile money account details, transaction records, and financial profile data, where this constitutes special personal data under applicable law
12. Racial or ethnic origin: not currently processed may be processed only where necessary for a specific, lawful purpose (e.g. diversity monitoring) with explicit consent
13. not currently processed may be processed only where necessary for a Genetic data: specific, lawful purpose with explicit consent
14. Political opinion: not currently processed may be processed only where necessary with explicit consent
15. Sexual life details: not currently processed may be processed only where necessary with explicit consent
16. Religious or philosophical beliefs: not currently processed may be processed only where necessary with explicit consent and
17. not currently processed may be processed only where Trade union membership: necessary with explicit consent.

Categories listed as "not currently processed" are included to ensure this Policy covers the Company's reasonably foreseeable activities. The Company will not commence processing of such categories without first establishing a lawful basis, conducting a necessity assessment, and updating this Policy and any required Data Protection Impact Assessment.

3.11 Transaction, Payment, and Metering Data

Transaction references, amounts, payment methods, and metadata for payments including mobile money (MoMo). Uploaded payment receipts and transaction IDs submitted through the recovery flow. Point Account balance, PointTransaction ledger entries (debits, credits, carry-forwards, refills, rollovers, gift transfers, reconstructions),

action and feature keys, installment-schedule nodes and status, milestone-compliance snapshots, and Refill Request records.

3.12 Communication and Engagement Data

Content of messages sent through the Platform's messaging features, AI Agent and assistant conversations, community posts and replies, screening threads, engagement messages, and conversion/gamification data (count of features activated and milestones reached aggregated, non-identifying counts, may be displayed as social proof individual activation data is not shown to other users).

4 HOW WE USE YOUR PERSONAL DATA

4.1 We process personal data for the following purposes:

18. Provision of services/products to customers: account management, financial tracking, property management, POS operations, payroll processing, AI-assisted tools, document and report generation, will and estate planning
19. Staff onboarding and human resource management: recruitment, onboarding, employment records, payroll, attendance, leave, performance management, disciplinary processes, security awareness training, and HR administration
20. Provision of mobile money services: MTN MoMo payment processing, transaction records, billing, installment schedules, and payment verification
21. Onboarding of students/pupils: AI Learner programme enrolment, training, certification, and educational content delivery
22. Supplier/contractor onboarding and management: supplier registration, procurement, contract management, purchase orders, goods receipt, and payment processing
23. General administration: account management, communication, in-app notifications, email, engagement messages, demand notes, receipts, reminders, and operational administration
24. Collection/processing required by law: compliance with Ugandan tax, employment, financial, property, and data protection laws as specified in Clause 5.1(c)
25. Security purposes: identity verification, document QR verification, sign-off recording, fraud prevention, anomaly detection, security awareness training, incident management, and audit trail maintenance

26. Cookies and website analytics: usage analytics, browsing history, device information, access times, pages viewed, and platform improvement

27. property rate and ground rent assessment, demand Performance of a public duty: note issuance, and collection on behalf of property owners and local authorities through the property management module

28. Advertising and referrals: display of advertisements, operation of the referral program, and the Conversion Psychology Engine (urgency campaigns, social-proof notifications, gamified milestones)

29. Billing and metering: Points conversion, installment schedules, milestone compliance, invoices, receipts, renewal enforcement, and auto-calibration of rates using aggregated, anonymised data and

30. export, sync, or publish data to Microsoft 365 Data integration and publishing: and social-media platforms the user has connected.

4.2 We do not process personal data for purposes that are incompatible with those for which the data was collected.

> *"We do not process personal data for purposes that are incompatible with those for which the data was collected."*
>
> **Clause 4.2 - Purpose Limitation**

5 LEGAL BASIS FOR PROCESSING

5.1 We process personal data on the following legal bases:

31. Consent: where the data subject has affirmatively consented (accepting Terms, enabling location capture, completing Mindcheck, opting in to marketing, subscribing to newsletters, connecting a third-party integration)

32. Contract: where processing is necessary to provide the Services the data subject has requested, including metering payable actions and enforcing billing cycles

33. where processing is required to comply with Ugandan law, Legal Obligation: including:

- Data Protection and Privacy Act, Cap. 97
- Constitution of the Republic of Uganda, 1995
- Income Tax Act, Cap. 338
- Value Added Tax Act, Cap. 344

- Accountants Act, Cap. 294
- Employment Act, Cap. 226
- National Social Security Fund Act, Cap. 230
- Companies Act, Cap. 106
- Contracts Act, Cap. 284
- Registration of Persons Act, Cap. 332
- Stamp Duty Act, Cap. 339
- Anti-Money Laundering Act, Cap. 118
- National Payments Systems Act, Cap. 59
- Computer Misuse Act, Cap. 96
- Electronic Signatures Act, Cap. 98
- Electronic Transactions Act, Cap. 99 and

34. Legitimate Interests: where processing is necessary for our legitimate interests in operating, securing, and improving the Platform, provided those interests do not override the data subject's rights and freedoms.

5.2 Where we rely on consent, the data subject may withdraw it at any time. Withdrawal does not affect the lawfulness of processing before the withdrawal.

> *"We do not sell personal data. We may share personal data with the following categories of recipients, and only to the extent necessary."*
>
> **Clause 6.1 – No Sale of Personal Data**

6 DATA SHARING AND DISCLOSURE

6.1 We do not sell personal data. We may share personal data with the following categories of recipients, and only to the extent necessary:

35. Service Providers: third parties acting on our behalf under confidentiality obligations (cloud hosting providers, email delivery services, payment processors, AI model providers)

36. Business and Module Members: within a business, property module, or POS module, data is shared with members according to the capabilities and access scope granted by the account owner

37. Employees: through the employee portal, employees access only their own payslips, leave, and attendance records
38. Advertisers: aggregated, non-identifying statistics regarding ad performance
39. Legal Authorities: where required by law, court order, or to protect the rights, property, or safety of the Company, our users, or the public and
40. Business Transfers: in connection with a merger, acquisition, or sale of all or part of our business, subject to confidentiality protections.

6.2 Multi-Tenant Data Isolation. Row-level security ensures that business, property module, and POS module data is scoped to the owning account. Members and team members may only access data within their assigned account and within their granted capabilities.

6.3 The Platform engages the following categories of sub-processors, each under confidentiality obligations: Base44 (cloud hosting), Resend (email delivery), MTN MoMo (mobile money payments), AI model providers (OpenAI, Google, Anthropic), and OAuth-connected services (Microsoft Outlook, Microsoft OneDrive, Google Drive, LinkedIn, Facebook Pages, Instagram Business). The full sub-processor register, including each provider's role, data categories processed, legal basis, and transfer destination, is maintained in Annex B: Sub-Processor Register.

6.4 Disclosure to Specific Persons and Bodies

6.4.1 In addition to the categories of recipients in Clause 6.1, the Company discloses personal data to the following specific persons and bodies, each for the stated purpose and only to the extent necessary:

Person / Body	Purpose for Disclosure
Uganda Revenue Authority	For tax purposes, including filing of tax returns, PAYE remittances, VAT declarations, and compliance with the Income Tax Act, Cap. 338 and the Value Added Tax Act, Cap. 344
Uganda Registration Services Bureau	For company registration and compliance with the Registration of Persons Act, Cap. 332 and the Companies Act, Cap. 106
Commercial Banks	For payment of staff salaries, processing of vendor payments, and management of the Company's banking transactions
National Social Security Fund	Provident fund for staff, including NSSF contributions and compliance with the National Social Security Fund Act, Cap. 230

Person / Body	Purpose for Disclosure
Education Institutions	For verification of academic documents submitted by recruitment candidates and employees, including transcripts, certificates, and qualifications
Telecom Companies	For provision of airtime and data benefits to staff, including mobile data bundles and communication allowances
Uganda Police Force	For investigation purposes, including reports of fraud, theft, cybercrime, or other criminal activity affecting the Company, its users, or its data
Donors	For funding and accountability purposes, including reporting on the use of funds, programme outcomes, and compliance with donor agreements

6.4.2 Disclosure to each person or body listed in Clause 6.4.1 is limited to the minimum personal data necessary for the stated purpose. The Company does not disclose personal data to any person or body beyond what is necessary for the purpose stated.

6.4.3 Where disclosure is made to a public body under a legal obligation, the Company relies on the legal bases set out in Clause 5.1(c). Where disclosure is made for a legitimate business purpose (e.g. salary payments to commercial banks, academic verification to education institutions), the Company relies on the legal bases set out in Clause 5.1(b) (Contract) or Clause 5.1(d) (Legitimate Interests), as applicable.

7 SPECIAL PERSONAL DATA

7.1 General Principles

7.1.1 The Company processes special categories of personal data - data relating to health, biometrics, financial information, racial or ethnic origin, genetic data, political opinion, sexual life, religious or philosophical beliefs, and trade union membership, as set out in Clause 3.10 - only where such processing is necessary, lawful, and accompanied by appropriate safeguards.

7.1.2 Where special personal data is processed based on consent, the data subject's consent must be explicit, affirmative, and specific to the category of data and the

purpose of processing. The data subject may withdraw consent at any time withdrawal does not affect the lawfulness of processing before the withdrawal.

The Company will not process special personal data for purposes incompatible

7.1 .3

with those for which it was collected. Where the Company intends to process a new category of special personal data not previously processed, it will conduct a Data Protection Impact Assessment, update this Policy, and obtain any necessary approvals before commencing processing.

7.2 Mindcheck (Health and Wellness Data)

7.2.1 Mindcheck collects data relating to mental and financial wellness, which constitutes sensitive personal data under the Data Protection and Privacy Act, 2019. We process this data only with the data subject's explicit, affirmative consent, given when they start the assessment.

Data subjects may complete Mindcheck without providing contact details results

7.2 .2

are shown regardless. Where an email is provided, and marketing opt-in is selected, we may send engagement and wellness content and subscribe the data subject to the Platform's newsletter.

7.2.3 We do not share individual Mindcheck responses, bands, or feedback with other users, advertisers, or third parties, except where required by law or with separate explicit consent. Only authorised administrators may access Mindcheck records for Platform operations, and only in aggregated or de-identified form for analytics.

7.2.4 Data subjects may withdraw Mindcheck consent at any time withdrawal does not delete historical records retained for legal or audit purposes.

7.3 Biometric Data

7.3.1 Biometric authentication data (WebAuthn/FIDO2 credentials) is processed for login and sensitive-action approvals across all account types (personal, business, property module, POS module, employee portal, and admin). Biometric templates are stored locally on the user's device the Company stores only the public key portion. Users may enroll and revoke biometric credentials at any time from their account Security settings.

7.3.2 Biometric data is processed based on the data subject's explicit consent, given when enrolling a biometric credential. The data subject may withdraw consent by revoking the credential at any time.

7.4 Other Special Personal Data

7.4.1 Where the Company processes any other category of special personal data listed in Clause 3.10, it will do so only where:

41. a lawful basis exists under the Data Protection and Privacy Act, 2019
42. the processing is necessary for the specified purpose
43. the data subject has been informed of the processing and
44. appropriate safeguards, including access controls, encryption, and minimisation, are in place.

7.4.2 The Company maintains a register of special personal data processing activities, which is reviewed as part of the annual policy review and whenever a new processing activity is contemplated.

8 MICROSOFT 365 AND THIRD-PARTY INTEGRATIONS

8.1 The Platform may integrate with Microsoft 365 (Outlook, OneDrive, Word, Excel) and other third-party services. When a data subject connects such an integration, their data is transferred to and processed by the third-party provider under that provider's terms and privacy policy.

8.2 Microsoft 365 data is processed and stored by Microsoft in data centres that may be located outside Uganda. By connecting a Microsoft 365 integration, the data subject consents to the international transfer of their data to Microsoft.

8.3 We process only the data necessary to perform the requested action. We do not retain Microsoft 365 credentials, and the data subject may disconnect an integration at any time.

Documents and files exported or archived are transferred to and

8.4 Google Drive.

stored by Google under Google's terms and privacy policy, potentially in data centres outside Uganda.

9 SOCIAL-MEDIA PUBLISHING

9.1 The Platform's automated social marketing engine may generate and publish content to connected social-media accounts (LinkedIn, Facebook, Instagram) on the data subject's behalf or on the Platform's behalf. Published content and account data are shared with the third-party social-media platform under its terms and privacy policy.

9.2 TikTok publishing is not automated the Platform stages draft content for manual posting, and no data is sent to TikTok without manual action.

9.3 A social-media integration may be disconnected at any time.

> *"We do not authorise AI model providers to use data for training their models."*
>
> **Clause 10.3 – AI Model Governance**

10 AI-ASSISTED PROCESSING

10.1 The Platform uses artificial intelligence to generate summaries, classifications, recommendations, financial digests, fuel-efficiency insights, Mindcheck guidance, marketing content, screening test questions, employee manual content, and other outputs based on user data.

10.2 When AI-assisted features are used, input data and relevant account data are sent to AI model providers for processing.

10.3 We do not authorise AI model providers to use data for training their models.

However, we cannot guarantee that AI model providers will not process data in ways outside our control.

10.4 AI-generated outputs are tools and do not constitute professional advice. Data subjects are responsible for reviewing and verifying all AI-generated content before acting on it.

11 DATA RETENTION

We retain personal data for as long as the account is active, or as long as necessary 11.1 to provide the Services.

11.2 After account closure or termination, we may retain data for a reasonable period to comply with legal obligations, resolve disputes, enforce agreements, and maintain audit trails.

11.3 Financial, property, tax, and accounting records may be retained for more than twenty (20) years to comply with Ugandan tax, accounting, property, and anti-money laundering laws, and to maintain audit trails, dispute resolution capabilities, and historical reference. This retention period may extend beyond account closure.

11.4 Archived account data is preserved in a read-only state and may be restored at the account owner's request or as required by law.

PointTransaction ledger entries, Refill

11.5 Metering and Transaction Records.

Request records, installment-schedule records, milestone-compliance snapshots, gift-transfer records, and renewal payment records are retained for the same period as financial and property records (up to ten (10) years).

11.6 Mindcheck Records. Mindcheck responses, bands, and feedback are retained for the period necessary to provide the Service and for Platform analytics. Data subjects may request erasure subject to legal retention obligations and the retention of de-identified, aggregated analytics.

Candidate data is retained for the recruitment cycle plus

11.7 Recruitment Records.

twelve (12) months after the hiring decision, after which it is deleted or anonymised.

Retention beyond this period may apply where required by law or for dispute resolution.

11.8 Specific retention periods for each data category are defined in the Platform's Data Retention Policy framework (Data Retention Policy entity) with automated retention enforcement. Financial, property, tax, and accounting records are retained for more than twenty (20) years to comply with Ugandan tax, accounting, property, and anti-money laundering laws. Recruitment records are retained for the recruitment cycle plus twelve (12) months. Mindcheck records are retained for the period necessary to provide the Service and for Platform analytics. The organisation will align all retention periods with the Data Protection and Privacy Regulations, 2021 and document them in a supplementary retention schedule.

12 DATA SECURITY

12.1 We implement appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, disclosure, or destruction, including encryption, access controls, row-level security, and regular security reviews.

Detailed measures are set out in our Information and Security Policy.

12.2 Document sign-off features create tamper-evident audit records, including the issuer's email, timestamp, and GPS location (when captured).

12.3 Sensitive data, including Mindcheck responses, is access-controlled so that only authorised administrators may view individual records, and analytics are produced in aggregated or de-identified form.

12.4 Despite our efforts, no system can be guaranteed to be perfectly secure. We will notify data subjects of any personal data breach affecting them where required by law.

> *"Data subject requests are responded to within one (1) month of receipt, in accordance with the Data Protection and Privacy Regulations, 2021."*
>
> **Clause 13.3 – Response Timeline**

13 DATA SUBJECT RIGHTS

13.1 Under the Data Protection and Privacy Act, 2019, data subjects have the following rights:

45. Right of Access: to request a copy of the personal data we hold about them

46. Right to Rectification: to request correction of inaccurate or incomplete personal data

47. Right to Erasure: to request deletion of personal data, subject to legal retention obligations

48. to receive personal data in a structured, machine- Right to Data Portability: readable format and transmit it to another controller

49. Right to Object: to object to processing for direct marketing or other purposes based on legitimate interests

50. Right to Restrict Processing: to request restriction of processing in certain circumstances and

51. Right to Withdraw Consent: to withdraw consent at any time where processing relies on consent.

To exercise these rights, data subjects contact us using the details in Clause 2.2.

13.2 We will respond within a reasonable time and may require verification of identity.

13.3 Data subject requests are responded to within one (1) month of receipt, in accordance with the Data Protection and Privacy Regulations, 2021. The Platform maintains a Data Subject Request handling system (Data Subject Request entity) through which requests are tracked to completion. The organisation acknowledges receipt of each request within seven (7) days and provides a substantive response within one month. Where necessary, based on the complexity of the request, the response period may be extended by a further two (2) months, with the data subject informed of the extension and the reasons within the first month.

14 COOKIES AND ELECTRONIC COMMUNICATIONS

14.1 The Platform uses local storage and similar technologies to remember preferences, maintain sessions, and provide a personalized experience. We do not use tracking cookies for third-party advertising.

By accepting the Terms and Conditions, data subjects consent to receive electronic 14.2 communications from us, including in-app notifications, email, and engagement messages, in accordance with the Electronic Transactions Act of Uganda.

Data subjects may opt out of non-essential communications at any time.

14.3

> *"The Company recognizes that the collection or processing of children's personal data requires a higher level of protection."*
>
> **Clause 15.1.1 – Heightened Protection**

15 PERSONAL DATA RELATING TO CHILDREN

15.1 General Position

The Company collects personal data relating to children in certain contexts as

15.1 .1

part of its operations. The Company recognizes that the collection or processing of children's personal data requires a higher level of protection, and appropriate security measures must be implemented to safeguard such data in accordance with the Data Protection and Privacy Act, 2019 and the Data Protection and Privacy Regulations, 2021.

15.1.2 The Company does not direct the Platform or its services at children, and children are not the primary target audience. However, children's personal data is collected in the following contexts:

52. the Mindcheck wellness assessment may collect personal data relating Mindcheck: to children, including when a parent or guardian completes a family wellness assessment that includes information about their children, or when a minor participates in the assessment with parental consent

53. Will and Estate Planning: minors named as beneficiaries, dependents, or heirs in wills, estate plans, insurance nominations, or other beneficiary arrangements managed by or through the Company

54. Next of Kin and Family Members: children's details provided as next of kin or family member information by adult data subjects

55. Dependents: dependent information provided for payroll, insurance, or administrative purposes and

56. any other circumstance where a child's personal data is Other Contexts: necessarily collected as part of the Company's operations.

15.2 Legal Basis and Purpose

15.2.1 The Company processes children's personal data on the following legal bases:

57. Parental Consent: carried out with the prior consent of the parent, guardian, or any other person having authority to make decisions on behalf of the child. This is the primary legal basis for processing children's personal data, including Mindcheck assessments involving minors and the inclusion of minor beneficiaries in wills and estate plans

58. where processing is necessary for the legitimate interests of Legitimate Interests: the Company or the adult data subject (e.g. administering a will or estate plan on

behalf of a parent who has named their minor child as a beneficiary), provided those interests do not override the child's rights and freedoms

59. Necessary to Comply with the Law: where processing is required to comply with applicable Ugandan law, including laws relating to estate administration, insurance, and tax and

60. Contract Performance: where processing is necessary for the performance of a contract to which the child is a party (with parental consent) or to take steps at the request of the child's parent or guardian before entering into a contract.

15.2.2 The Company does not process children's personal data for purposes incompatible with those for which it was collected. The Company does not use children's personal data for direct marketing, profiling, or automated decision-making.

15.3 Safeguards for Children's Data

15.3.1 Where the Company processes children's personal data, it implements the following heightened safeguards:

61. Data Minimisation: only the minimum data necessary for the specific purpose is collected and retained

62. Access Controls: children's data is subject to the same or stricter access controls as special personal data, with access limited to authorised administrators

63. No Marketing or Profiling: the Company does not use children's personal data for marketing, advertising, profiling, or automated decision-making

64. the Company does not send direct marketing or No Direct Communication: engagement communications to children

65. Retention Limits: children's data is retained only for as long as necessary for the specific purpose for which it was collected, and is deleted or anonymised when no longer required

66. Parental Rights: parents or guardians may exercise data subject rights on behalf of their children, including access, rectification, erasure, and objection, using the contact details in Clause 2.2 and

67. Breach Notification: any personal data breach affecting children is treated as high-risk and notified to the PDPO and affected data subjects without undue delay.

15.4 Unauthorised Collection

15.4.1 If the Company becomes aware that it has collected personal data from a child without verifiable parental consent in a context where such consent was required, it will take reasonable steps to delete that data, unless retention is required by law.

15.4.2 The Company does not knowingly process special categories of personal data relating to children (e.g. health, biometric, or genetic data) except where strictly necessary and with appropriate parental consent and safeguards. Mindcheck assessments involving minors require explicit parental consent and are subject to the heightened safeguards in Clause 15.3.

15.5 Review and Compliance

15.5.1 The Company reviews its children's data handling practices as part of the annual policy review and whenever a new processing activity that may involve children's data is contemplated.

Where the Company intends to introduce services directed at or likely to be

15.5 .2

accessed by children, it will conduct a Data Protection Impact Assessment specific to children's data, update this Policy, and implement age-appropriate safeguards before commencing such services.

16 INTERNATIONAL DATA TRANSFERS

16.1 Personal data is primarily stored and processed in data centres that may be located outside Uganda. By using the Platform, data subjects consent to the transfer of their personal data to such countries.

16.2 Where data is transferred outside Uganda — including to Microsoft 365, Google Drive, social-media platforms, AI model providers, and other service providers - we take reasonable steps to ensure it is protected by appropriate safeguards, such as standard contractual clauses or equivalent protections.

16.3 The following table sets out each country to which personal data is transferred, the purpose of the transfer, and the description of personal data being transferred:

#	Country	Purpose of Transfer	Description of Personal Data Being Transferred
1	United States of America	Cloud hosting and platform infrastructure (Base44)	All platform data: account records, identifiers (name, email, phone, national ID), financial data (income, expenses, assets, savings, loans, budgets), property data, POS data, business data, employee records, payroll, recruitment records, blog content, community posts, Mindcheck responses, biometric credential public keys, document attachments, audit logs, and system configuration
2	United States of America	AI-assisted processing (OpenAI, Google, Anthropic)	User prompts, account data context, financial summaries, CV data, screening test inputs, Mindcheck inputs, blog content for generation, marketing content briefs, document text for extraction, and support messages - sent to AI model providers for processing and returned as AI- generated outputs
3	Europe (Netherlands)	Email delivery and transactional email (Resend)	Email addresses, email subject lines, email body content (welcome emails, OTP codes, password reset links, engagement messages, demand notes, receipts, recruitment reminders, newsletter content, and notification emails), and email metadata (delivery status, open/click tracking)
4	Global (Microsoft data centres)	Microsoft 365 integration - Outlook, OneDrive, Word, Excel (when user	Email messages, calendar events, contacts, documents, spreadsheets, and

#	Country	Purpose of Transfer	Description of Personal Data Being Transferred
		connects)	files exported or archived by the
			user to Microsoft 365 services. Data is transferred at the user's request when they connect a Microsoft integration
5	Global (Google data centres)	Google Drive integration (when user connects)	Documents and files exported or archived by the user to Google Drive. Data is transferred at the user's request when they connect a Google Drive integration
6	Global (LinkedIn data centres)	LinkedIn social-media publishing (when user connects)	Marketing post content, post text, hashtags, and account profile data. Data is transferred at the user's request when they connect a LinkedIn integration
7	Global (Meta/Facebook data centres)	Facebook Pages and Instagram Business publishing (when user connects)	Marketing post content, post text, images, videos, and page/account profile data. Data is transferred at the user's request when they connect a Facebook or Instagram integration

16.4 The full transfer mapping, including specific safeguards in place for each transfer (e.g. standard contractual clauses or equivalent protections), is maintained in Annex B:

Sub-Processor Register. The Company will execute Data Processing Agreements with each sub-processor before formal approval of this Policy.

Data transferred to Uganda (MTN MoMo mobile money payments) is a domestic 16.5 transfer within Uganda and is not an international transfer. MTN MoMo processes payment data within Uganda under the National Payments Systems Act, Cap. 59.

17 AGGREGATED AND ANONYMISED DATA

17.1 We may collect, use, and share aggregated or anonymised data that does not identify individuals - such as usage statistics, platform performance metrics, fuel-rate calibration data, conversion-engine social-proof counts, Mindcheck aggregate statistics, and sector-wide trends - for analytics, improvement, and marketing purposes.

17.2 Once data is anonymised, it is no longer personal data and is not subject to the rights in Clause 13.

18 PERSONAL DATA BREACH NOTIFICATION

18.1 In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of data subjects, we will notify the affected data subjects and the Personal Data Protection Office (PDPO) without undue delay and in accordance with the timelines prescribed by the Data Protection and Privacy Act, 2019 and the Data Protection and Privacy Regulations, 2021.

18.2 Internal breach assessment procedures, notification decision matrix, and responsible personnel for PDPO and data subject notification are documented in Annex A: Incident Response Plan. The Security Incident system provides the operational workflow for breach assessment, PDPO notification tracking (pdpo_notifiable, pdpo_notified_at), and data subject notification (subjects_notified_at).

19 CHANGES TO THIS POLICY

19.1 We may update this Policy from time to time to reflect changes in our practices, legal requirements, or Platform features.

19.2 When we make material changes, we will update the "Last Updated" date and notify data subjects through the Platform or by email.

20 COMPLAINTS

20.1 If a data subject believes we have not complied with this Policy or applicable data protection laws, they may lodge a complaint with us using the contact details in Clause

2.2 .

20.2 Data subjects also have the right to lodge a complaint with the Personal Data Protection Office (PDPO) of Uganda.

21 APPROVAL AND SIGNATURE

This Data Protection and Privacy Policy has been approved by the Director of **Torrid Petric Legacy Enterprises Ltd**. It takes effect on the effective date recorded below and remains in force until superseded or withdrawn. The approval details and authorized signature below confirm its formal adoption.

Field	Value
Approved by	SSENKUMBA PATRICK
Title	Director, **Torrid Petric Legacy Enterprises Ltd**

APPROVED AND SIGNED

