PRIVACY & COOKIE POLICY

(Including Exhibit 1 – Cookie Notice)

1. PREAMBLE

1.1 General Declaration

1.1.1 Policy Adoption and Corporate Standing

1.1.1.1 This Privacy & Cookie Policy (hereinafter sometimes referred to, inter alia, as the "Policy") is a document of binding legal effect and interpretive authority, adopted, executed, published and promulgated by SellMMO Group FZ LLE, Fujairah Creative City Free Zone, License No. 14608/2019, P.O. Box 4422, United Arab Emirates, a juridical person duly incorporated, validly existing and in good standing under the laws of the United Arab Emirates, specifically within the Fujairah Creative City Free Zone, situated in the Creative Tower, Emirate of Fujairah, United Arab Emirates.

1.1.1.2 The Company acts, mutatis mutandis, in its capacity as an Aggregator, escrow facilitator and technical operator of affiliated Storefronts, rather than as a direct seller of digital goods, together with its Affiliates, Subsidiaries and duly authorised successors or assigns (collectively, the "Company" or the "Group").

1.1.2 Purpose and Public Character

1.1.2.1 This Policy constitutes the principal privacy charter of the Company and its Group, articulating the principles by which all Personal Data and related information are collected, processed, stored, shared, safeguarded and ultimately disposed of.

1.1.2.2 It serves as a public declaration of the Company's commitment to lawful, transparent, and accountable data governance, forming part of the Group's broader compliance and governance framework, together with its other public-facing terms and policies governing user relations, payment security, financial crime prevention, and information protection.

1.2 Legal Basis and Interpretive Framework

1.2.1 Applicable Instruments

1.2.1.1 This Policy shall be construed, mutatis mutandis, in light of, and consistently with, the following legislative instruments of data protection law, as amended from time to time:

(a) Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data of the United Arab Emirates (the "UAE PDPL");

(b) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "EU GDPR");

(c) United Kingdom Data Protection Act 2018 and United Kingdom General Data Protection Regulation (the "UK GDPR"); and

(d) United States state privacy statutes, including without limitation the California Consumer Privacy Act of 2018 as amended by the California Privacy Rights Act of 2020 (the "CPRA"), the Virginia Consumer Data Protection Act (the "VCDPA"), the Colorado Privacy Act (the "CPA"), the Connecticut Data Privacy Act (the "CTDPA"), the Utah Consumer Privacy Act (the "UCPA"), and any analogous enactments.

1.2.2 Interpretive Clause

1.2.2.1 Provided however that nothing herein shall be deemed to waive, diminish or derogate from any mandatory provision of Applicable Law.

1.2.2.2 In the event of any conflict or inconsistency among the above frameworks, the interpretation most protective of the Data Subject and most compliant with the strictest jurisdictional standard shall prevail.

1.3 Corporate Philosophy and Principles

1.3.1 Recognition of Fundamental Rights

1.3.1.1 The Company recognises, affirms and declares that the rights of natural persons to privacy, dignity and informational self-determination are paramount, subject always to legitimate business interests, compliance obligations, and statutory duties.

1.3.2 Ethical Governance Commitment

1.3.2.1 The Company conducts its affairs in accordance with principles of good governance, accountability, transparency and proportionality, seeking to maintain equilibrium between operational necessity and the protection of individual rights.

1.3.2.2 Accordingly, this Policy is issued as a living instrument of accountability and a manifestation of the Group's adherence to best practices in privacy management, risk oversight, and lawful data stewardship.

1.4 Structure and Overview of the Policy

1.4.1 Structural Outline

1.4.1.1 For the convenience of the reader and to facilitate systematic interpretation, this Policy is structured into sequentially numbered sections and annexes, each serving a defined legal and operational function:

(a) Section 1 – Preamble: establishes the legal authority, interpretive context, and guiding philosophy of the Company's privacy regime.

(b) Section 2 – Scope; Controller Identity; Contact: defines the entities and territorial scope to which the Policy applies and sets out primary contact channels.

(c) Section 3 – Categories of Data and Sources: enumerates data types and lawful acquisition sources.

(d) Section 4 – Purposes and Legal Bases: specifies lawful grounds for Processing activities.

(e) Section 5 – Cookies and Tracking Technologies: sets forth principles of online tracking, with reference to Exhibit 1 – Cookie Notice (Meduza Services / PayTabs Gateway).

(f) Section 6 – Special Categories and Children's Data: describes restrictions concerning sensitive data and minors.

(g) Section 7 – Disclosures; Processors; Third-Party Links: lists authorised recipients, contractual safeguards, and interoperability with external environments.

(h) Section 8 – International Transfers: details transfer mechanisms and protective clauses.

(i) Section 9 – Retention and Deletion: summarises retention criteria and deletion practices.

(j) Section 10 – Security Measures: outlines high-level technical and organisational protections.

(k) Section 11 – Data Subject Rights: explains individual entitlements and submission channels.

(l) Section 12 – Breach Notification: establishes notification procedures and limitations.

(m) Section 13 – Liability and Disclaimers: sets boundaries of corporate responsibility.

(n) Section 14 – Governing Law and Jurisdiction: identifies controlling law and forum.

(o) Section 15 – Changes; Entire Agreement: governs amendments and publication; includes Section 15.3 (Voluntary Choice of Buyer) addressing buyer autonomy and assumption of risk.

(p) Section 16 – Physical Merchandise & Fulfilment Partners: describes roles, disclosures, legal bases, retention, and liability in connection with physical goods.

(q) Annex A – Definitions (Full List); Annex B – Regional Contacts & Representatives; Annex C – International Transfers & Processor Terms; and Exhibit 1 – Cookie Notice.

1.4.2 Integration with Corporate Framework

1.4.2.1 This Policy is to be read in pari materia with the Company's other publicly available instruments forming the SellMMO Group compliance corpus, including (without limitation) the Terms of Service, Refund & Buyer Protection Policy, Delivery & Fulfilment Policy, Return & Warranty Policy, Escrow & Payment Policy, and Sanctions & Fraud Compliance Statement, as each may be amended or updated from time to time.

1.4.2.2 Each instrument addresses a distinct operational domain, yet all operate cumulatively to ensure a single, coherent, and enforceable compliance architecture.

1.5 Statement of Commitment

1.5.1 Guiding Intent

1.5.1.1 In promulgating this Policy, the Company underscores its conviction that responsible data management constitutes both a legal obligation and a moral imperative.

1.5.1.2 The Company shall at all times strive to:

(a) uphold the highest attainable standards of privacy governance;

(b) maintain transparency toward users, partners and regulators;

(c) balance lawful business conduct with the fundamental rights of individuals; and

(d) continuously assess and improve internal safeguards in line with evolving legislation and technology.

1.5.2 Binding Effect

1.5.2.1 For the avoidance of doubt, this Policy represents a binding public statement of principles, compliance posture and accountability mechanisms by which the Company and its personnel shall be guided in all matters pertaining to the Processing of Personal Data.

1.5.2.2 Any deviation from these principles shall be construed narrowly and only to the extent necessary to comply with mandatory legal obligations or to protect the vital interests of the Company and its users.

1. DEFINITIONS

1.1 General Clause

1.1.1.1 For the avoidance of doubt, the following terms, when capitalised and used herein, shall bear the meanings assigned below.

1.1.1.2 Words importing the singular include the plural and vice versa; words importing any gender include all genders; and references to legal instruments or authorities shall be construed as references to such instruments or authorities as amended, replaced, supplemented or restated from time to time.

1.2 Defined Terms

1.2.1 “Applicable Law”

1.2.1.1 “Applicable Law” shall mean, collectively and severally, all statutes, legislative instruments, executive regulations, regulatory guidance, decrees, circulars, judicial precedents and administrative practices governing or relevant to the Processing of Personal Data.

1.2.1.2 Such laws shall include, mutatis mutandis, the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data (UAE PDPL), the EU General Data Protection Regulation (EU GDPR), the UK GDPR and Data Protection Act 2018, and the principal U.S. state privacy statutes (including the CPRA, VCDPA, CPA, CTDPA, UCPA), together with any analogous laws of jurisdictions in which Data Subjects are located.

1.2.1.3 All such instruments shall, mutatis mutandis, govern the interpretation and application of this Policy to the extent they apply to the Company’s operations, without derogation from any mandatory right or duty under law.

1.2.2 “Controller”

1.2.2.1 “Controller” shall mean that natural or legal person which, alone or jointly with others, determines the purposes and essential means of Processing of Personal Data.

1.2.2.2 For the avoidance of doubt, the Company shall ordinarily act as Controller in relation to Personal Data processed within or through its platforms, except where it operates as Joint Controller or Processor under a specific commercial arrangement, as further described in Section 2 (Scope; Controller Identity; Contact).

1.2.3 “Processor”

1.2.3.1 “Processor” shall mean any natural or legal person, public authority, agency or other body that Processes Personal Data on behalf of the Controller, under a written data-processing agreement imposing confidentiality, security and compliance obligations that are no less protective than those required by Applicable Law.

1.2.3.2 Such agreements (Data Processing Agreements, “DPAs”) shall, inter alia, ensure adherence to recognised international standards, proportionality of Processing, and effective oversight by the Controller.

1.2.4 “Personal Data”

1.2.4.1 “Personal Data” shall mean any information relating to an identified or identifiable natural person (a “Data Subject”), including, without limitation, name, alias, account identifier, email

address, device or IP address, transactional records, cookies, geo-location signals, payment identifiers, or any data that directly or indirectly enables the identification of such person.

1.2.4.2 Provided however that anonymised, aggregated, or de-identified data—duly established as such under Applicable Law and maintained in a form that no longer permits re-identification—shall not be deemed Personal Data.

1.2.5 “Processing”

1.2.5.1 “Processing” shall mean any operation or set of operations performed upon Personal Data, whether or not by automated means, including, inter alia, collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, alignment, restriction, erasure or destruction.

1.2.5.2 The term shall be interpreted broadly and in accordance with the protective purpose of Applicable Law.

1.2.6 “International Transfer”

1.2.6.1 “International Transfer” shall mean any transmission, routing, disclosure or making available of Personal Data to a jurisdiction other than that in which the data originated, including transfers to countries or territories not recognised as providing an adequate level of protection.

1.2.6.2 Provided always that any such transfer shall occur only under lawful mechanisms affording appropriate safeguards, as described in Annex C (International Transfers & Processor Terms), including but not limited to Standard Contractual Clauses, UK Addenda, the Data Privacy Framework, or contractual equivalents recognised under the UAE PDPL.

1.2.7 “Data Subject”

1.2.7.1 “Data Subject” shall mean any identified or identifiable natural person whose Personal Data is processed by or on behalf of the Company, including but not limited to Buyers, Sellers, Influencers, Visitors, or representatives of business partners.

1.2.8 “Company”, “Group”, or “SellMMO Group FZ LLE”

1.2.8.1 These terms shall be construed interchangeably to denote the legal entity SellMMO Group FZ LLE, together with its affiliates and subsidiaries acting under its lawful control or instruction, as described in the Preamble.

1.2.9 “Annexes and Exhibits”

1.2.9.1 References to Annex A (Definitions – Full List) shall include additional defined terms used across the Group’s documentation, such as “Affiliate,” “Subsidiary,” “Special Categories of Data,” “Sensitive Personal Information,” and “Sale/Share” under U.S. privacy statutes.

1.2.9.2 All such annexes and exhibits shall be read in pari materia with this Policy and form an integral, legally binding part hereof.

1.3 Interpretive Principle

1.3.1 Where terms are undefined in this Policy, they shall bear their meaning under Applicable Law or, where context requires, their ordinary and natural meaning consistent with industry usage.

1.3.2 Headings and numbering are for convenience only and shall not affect interpretation.

2. SCOPE; CONTROLLER IDENTITY; CONTACT

2.1 Scope

2.1.1 General Applicability

2.1.1.1 Subject always to Applicable Law and notwithstanding any contrary custom or practice, this Policy applies to all acts or omissions constituting the Processing of Personal Data by or on behalf of the Company, whether directly or indirectly, by automated means or otherwise.

2.1.1.2 Such Processing extends to activities connected with the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces ("APIs"), influencer and/or affiliate programmes, and any ancillary or successor services or functionalities (collectively, the "Services").

2.1.2 Extraterritorial Reach

2.1.2.1 Without prejudice to the generality of the foregoing, this Policy applies to Processing activities that fall within the territorial scope of the UAE PDPL, EU GDPR, UK GDPR, and analogous U.S. state privacy statutes (including CPRA, VCDPA, CPA, CTDPA, UCPA).

2.1.2.2 Provided however that compliance therewith shall be interpreted subject to conflicts-of-law principles and mandatory local public policy.

2.1.3 Carve-Outs and Precedence

2.1.3.1 This Policy does not apply to:

(a) information that has been rendered anonymised or aggregated in accordance with Applicable Law;

(b) information expressly excluded from data-protection statutes (e.g., journalistic, academic or household activities); or

(c) Processing performed by the Company solely as a Processor/Service Provider/Contractor on behalf of enterprise clients under a data processing agreement ("DPA").

2.1.3.2 In such cases, the terms of the relevant DPA and any lawful transfer mechanisms (e.g., SCCs, UK IDTA/Addendum, DPF) shall prevail inter se, subject always to mandatory duties retained by the Company as Controller for residual Processing.

2.1.4 Sectoral and HR Data

2.1.4.1 Processing relating to employment or personnel records, whistle-blower channels, and vendor due diligence may be governed by separate privacy notices (each an "Ancillary Notice").

2.1.4.2 Such Ancillary Notices shall, save where prohibited by law, be read in pari materia with this Policy; in case of conflict, the more specific notice shall prevail.

2.1.5 Hierarchy and Language

2.1.5.1 In the event of conflict between this Policy and any annex, schedule or exhibit, the latter shall prevail only in respect of the subject matter it specifically addresses.

2.1.5.2 Translations are provided for convenience; the English version shall be authoritative except where local law mandates otherwise.

2.1.6 Current-Version Clause

2.1.6.1 References in this Policy to other Company Policies, Annexes or Exhibits shall be construed to mean the current, duly approved and most recently published version thereof.

2.1.6.2 Such version shall prevail in the event of any dispute or inconsistency, save where Applicable Law requires otherwise.

2.2 Controller Identity and Role Allocation

2.2.1 Primary Controller

2.2.1.1 SellMMO Group FZ LLE, Fujairah Creative City Free Zone, License No. 14608/2019, P.O. Box 4422, United Arab Emirates, shall, unless expressly stated otherwise, act as the Controller for Processing undertaken for the purposes set out in Section 4 (Purposes and Legal Bases).

2.2.2 Joint Controllers and Delegated Operations

2.2.2.1 For certain modalities of the Services — including hosted or white-label storefronts operated for Influencers or Affiliates, marketplace integrations, escrow confirmations, and anti-fraud shared services — the Company may act either:

(a) as a Joint Controller together with a partner platform; or

(b) as a Processor strictly limited to documented instructions.

2.2.2.2 The allocation of roles and liabilities shall be defined in the relevant commercial agreements and regional addenda and interpreted in pari materia with the Company's internal compliance standards.

2.2.3 EU/UK Representatives (Art. 27 GDPR/UK GDPR)

2.2.3.1 Where the Company lacks an establishment within the EEA and/or the UK but falls within GDPR Art. 3(2) or UK GDPR Art. 3(2), it shall designate an EU and/or UK Representative for the limited purpose of Art. 27, whose particulars are set forth in Annex B (Regional Contacts & Representatives).

2.2.4 U.S. Role Equivalents

2.2.4.1 For U.S. state privacy laws, references to Controller and Processor shall be interpreted, mutatis mutandis, as Business and Service Provider/Contractor, without prejudice to any contrary definition under Applicable Law.

2.2.5 Sub-Processors and Onward Transfers

2.2.5.1 The Company may engage vetted Processors or Sub-Processors for hosting, payment processing, risk scoring, analytics and support services, under written DPAs imposing obligations no less protective than those mandated by Applicable Law.

2.2.5.2 A high-level summary of transfer mechanisms (including SCCs, UK Addenda and DPF participation where applicable) is set forth in Annex C (International Transfers & Processor Terms).

2.2.6 Ultimate Responsibility

2.2.6.1 Notwithstanding any delegation or appointment of a Representative, the Company remains responsible, to the extent mandated by Applicable Law, for ensuring that Processing on its behalf is conducted in accordance with this Policy and Applicable Law.

2.2.6.2 Provided however that nothing herein shall extend liability beyond what is imposed by statute or by contract.

2.3 Contact; Data Subject Requests; Agents and Appeals

2.3.1 Primary Contact Channels

2.3.1.1 Data Subjects may contact the Company via privacy@sellmmo.com

or by written correspondence to the registered address indicated in Annex B.

2.3.1.2 The Company may, at its discretion and subject to verification, make available a web form for Data Subject Access Requests ("DSARs").

2.3.2 DPO and Regional Points of Contact

2.3.2.1 Where required under Applicable Law, the Company shall designate a Data Protection Officer ("DPO") and/or EU/UK Representative(s); their details are listed in Annex B.

2.3.2.2 Communications shall be deemed received upon actual receipt; statutory response periods shall commence only after successful verification of the requester's identity.

2.3.3 Verification and Response Timeframes

2.3.3.1 The Company shall respond to verified DSARs without undue delay and within:

(a) one (1) month under the GDPR/UK GDPR (extendable by up to two (2) months for complex requests);

(b) a reasonable period under the UAE PDPL, having regard to complexity and volume; and

(c) forty-five (45) days under U.S. state privacy laws (extendable once by a further forty-five (45) days where necessary).

2.3.4 Authorised Agents and Appeals

2.3.4.1 Where permitted, Data Subjects may act through an Authorised Agent upon verification of authority and identity.

2.3.4.2 In jurisdictions providing a statutory appeal process, the Company shall offer a means to appeal refusals within the prescribed period and shall inform the Data Subject of the outcome and further recourse.

2.3.5 Opt-Out Preference Signals and Do Not Track

2.3.5.1 Subject to technical feasibility and legal mandate, the Company shall make reasonable efforts to detect and honour recognised Opt-Out Preference Signals (e.g., Global Privacy Control, Universal Opt-Out Mechanisms endorsed in Colorado) for targeted advertising and certain data "sales/shares," as further explained in Exhibit 1 — Cookie Notice.

2.3.5.2 Industry "Do Not Track" signals are not treated as legally binding requests unless standardised by law; nonetheless, the Company shall honour legally recognised Opt-Out Preference Signals where required.

2.3.6 Form and Language of Requests

2.3.6.1 DSARs may be submitted in English or another official language of the relevant jurisdiction as required by law; processing timelines run from receipt of a version intelligible to the Company.

2.4 Aggregator Role Disclaimer

2.4.1 The Company acts solely as an Aggregator and technical facilitator, transmitting payments and orders between Buyers and independent third-party sellers, fulfilment partners or influencers.

2.4.2 The Company does not create, own or control the underlying digital or in-game items and assumes no responsibility for their legality, quality, availability or functionality.

2.4.3 All obligations related to such goods or services rest exclusively with the respective third parties. See also Sections 7.5, 13.5 and 15.3 for further limitations and disclaimers applicable to third-party marketplaces and game-publisher enforcement.

3. CATEGORIES OF PERSONAL DATA; SOURCES

3.1 Categories of Personal Data

3.1.1 Identity and Contact Data

3.1.1.1 Includes, inter alia, names, aliases, postal and billing addresses, email addresses, telephone numbers, and government-issued identifiers (such as passport numbers, Emirates ID, national insurance numbers), together with demographic information (date of birth, nationality, gender).

3.1.1.2 Subject always to limitations under GDPR Art. 9 and UAE PDPL Art. 5 where such data constitute Special Categories or Sensitive Personal Information.

3.1.2 Account and Transaction Data

3.1.2.1 Records pertaining to the creation, maintenance and use of user accounts, login credentials, purchase and sales history, escrow confirmations, refunds and invoices, and other information necessary for the execution of contractual obligations.

3.1.2.2 Retention thereof shall be limited to statutory and legitimate business requirements and, upon expiry of the applicable period, the data shall be securely deleted or anonymised, as set out in Section 9 (Retention & Deletion).

3.1.3 Payment Instrument Tokens

3.1.3.1 Tokenised or pseudonymised identifiers generated by Payment Service Providers (“PSPs”), including card tokens, virtual account numbers, IBAN surrogates, and authorisation references.

3.1.3.2 The Company does not store raw cardholder data (e.g., PAN, CVV/CVC, track data); payments are processed exclusively through PCI-DSS-validated environments of its authorised PSPs (inter alia, PayTabs).

3.1.3.3 Only transaction metadata (amount, date, merchant identifier, status codes) may be retained for audit and anti-fraud purposes.

3.1.4 Technical and Usage Data

3.1.4.1 Information collected via devices and applications, including IP addresses, cookies, SDKs, telemetry signals, session logs, browser type, operating system, time zones, referrer URLs, and advertising identifiers.

3.1.4.2 This includes analytics and performance metrics from Meduza Services, and limited diagnostic logs from PSP-hosted pages (e.g., PayTabs Gateway).

3.1.4.3 Further details on cookies, pixels and SDK identifiers are set forth in Exhibit 1 — Cookie Notice.

3.1.5 Marketing and Communications Preferences

3.1.5.1 Records of opt-ins, opt-outs, consent withdrawals, language preferences, advertising segments, hashed identifiers used for targeted advertising, and communications logs.

3.1.5.2 Such Processing is subject to Data Subject rights (Section 11) and, where legally mandated and technically feasible, shall be suppressed upon valid detection of Global Privacy Control (GPC) or Universal Opt-Out Mechanism (UOOM) signals, without prejudice to Essential Cookies.

3.1.6 User-Generated and Support Content

3.1.6.1 Content voluntarily provided by Data Subjects through forums, reviews, support tickets, or communications channels ("UGC").

3.1.6.2 Such content may contain Personal Data which shall be moderated, stored, and deleted in accordance with Section 9 (Retention & Deletion), subject to Applicable Law and the principles of data minimisation and purpose limitation.

3.1.7 Fraud Prevention and Risk Signals

3.1.7.1 Behavioural patterns, device fingerprints, velocity checks, blacklist and whitelist identifiers, sanctions-list matches, chargeback data and risk scores used to detect and prevent fraudulent or unlawful activities.

3.1.7.2 All such Processing is conducted under proportionality and necessity principles and retained for periods strictly required by Applicable Law and risk-management standards.

3.1.8 Affiliate and Referral Tracking Data

3.1.8.1 Cookie identifiers, referral links, influencer codes, click-through records, and associated metadata collected solely for attribution of traffic and commission settlement, performance analytics, and fraud verification.

3.1.8.2 Such Processing remains subject to Applicable Law and consent mechanisms described in Section 4 (Purposes and Legal Bases) and Section 5 (Cookies and Tracking).

3.1.9 Hosted PSP and Third-Party SDK Signals

3.1.9.1 Limited identifiers and telemetry collected on PSP-hosted payment pages or within third-party SDKs (e.g., analytics or engagement tools provided by Meduza or PayTabs).

3.1.9.2 Such data are governed by the respective providers' privacy terms and lie outside the Company's direct technical control.

3.1.9.3 Disclosures and consent are surfaced to users where feasible and otherwise governed by those providers' mechanisms as set forth in Exhibit 1 — Cookie Notice.

3.1.10 In-Game Account and Fulfilment Data

3.1.10.1 Buyer-supplied identifiers strictly necessary for digital delivery (e.g., character name, realm/shard, guild, in-game mail handle), delivery method details (direct trade, mail, auction, guild bank) and Proof-of-Fulfilment records.

3.1.10.2 For the avoidance of doubt, passwords, security answers and complete credential sets are neither requested nor stored by the Company.

3.1.10.3 Classifications of prohibited or restricted identifiers or activities shall follow the Company's current internal compliance standards and applicable laws, as reflected in the most recently published public guidance on prohibited or restricted uses available on the Company's official website.

3.2 Sources of Personal Data

3.2.1 Direct Collection

3.2.1.1 Personal Data is obtained directly from Data Subjects when they register accounts, complete transactions, communicate with support, or otherwise interact with the Services.

3.2.2 Automated Collection

3.2.2.1 Data is automatically collected through cookies, pixels, SDKs, telemetry modules and similar technologies, subject to consent requirements under GDPR/ePrivacy/UK PECR and opt-out rights under U.S. State Privacy Laws.

3.2.2.2 The Company relies on its analytics partner Meduza Services for telemetry and on PayTabs Gateway for payment sessions and fraud-detection telemetry, each operating under its own lawful basis and technical environment as disclosed in Exhibit 1.

3.2.3 Third-Party Processors and Service Providers

3.2.3.1 Includes payment gateways, analytics providers, fraud-prevention vendors, logistics partners and communication platforms, each bound by written DPAs or equivalent instruments consistent with Annex C (International Transfers and Processor Terms).

3.2.4 Public and Partner-Provided Sources

3.2.4.1 Data may be obtained from public registers, sanctions lists, social-media platforms (where permitted), business partners and affiliates, subject to Applicable Law and transparency requirements.

4. PURPOSES & LEGAL BASES

4.1 Purposes of Processing

4.1.1 Provision of Services

4.1.1.1 To furnish, operate, and maintain the Services, including, inter alia, hosted storefronts, programmatic interfaces ("APIs"), and associated functionalities.

4.1.1.2 Processing under this purpose includes routing of requests between storefronts, integration with third-party marketplaces, and coordination with escrow and payment systems, subject always to the Terms of Service and applicable commercial agreements.

4.1.2 Account Administration

4.1.2.1 To create, manage, authenticate, suspend, terminate, or otherwise administer user accounts, including credential resets and fraud lockouts, and to maintain account integrity through identity-verification and access-management controls.

4.1.3 Order Fulfilment and Escrow Confirmations

4.1.3.1 To process, validate, and fulfil orders; confirm escrow releases from external peer-to-peer marketplaces; and provide receipts and delivery confirmations.

4.1.3.2 Processing includes reconciliation of Proof-of-Fulfilment records, log verification, and correspondence with relevant counterparties, consistent with consumer-protection requirements.

4.1.4 Payments and Payouts

4.1.4.1 To process incoming and outgoing payments, execute refunds and chargebacks, and perform reconciliations using tokenised identifiers supplied by Payment Service Providers ("PSPs").

4.1.4.2 For the avoidance of doubt, the Company does not collect, store, or otherwise process raw cardholder data (PAN, CVV/CVC, track data).

4.1.4.3 All payment credentials are handled exclusively through PayTabs Gateway or equivalent PSPs within a PCI-DSS-validated hosted environment.

4.1.4.4 The Company operates an escrow mechanism that temporarily holds funds until Buyer confirmation of delivery, solely to mitigate fraud risk and ensure equitable settlement.

4.1.5 Fraud Detection and Risk Management

4.1.5.1 To detect, investigate, and mitigate potentially fraudulent or abusive activity, including the use of device fingerprints, velocity checks, sanctions-list screening, and blacklist/whitelist analytics.

4.1.5.2 Such Processing is proportionate, minimised, and performed under contractual and statutory safeguards consistent with AML & CFT obligations.

4.1.6 Security

4.1.6.1 To ensure confidentiality, integrity, and availability of systems and data through logging, intrusion detection, penetration testing, access control, encryption, and incident-response measures.

4.1.6.2 This includes security telemetry collected via Meduza Services SDK and server monitoring modules.

4.1.7 Compliance with Legal Obligations

4.1.7.1 To comply with mandatory requirements under Applicable Law, including anti-money-laundering (AML), counter-terrorist-financing (CFT), sanctions screening, taxation, accounting, and lawful requests from competent authorities.

4.1.7.2 Such Processing is performed to the extent strictly required by statute and retained in accordance with prescribed limitation periods.

4.1.8 Analytics and Service Improvement

4.1.8.1 To collect aggregate metrics, perform quality assurance, optimise user experience and platform efficiency, and develop new functions.

4.1.8.2 Provided however that such Processing is subject to data-minimisation and pseudonymisation principles, and relies on analytics instrumentation provided by Meduza Services, as detailed in Exhibit 1 – Cookie Notice.

4.1.9 Marketing and Communications

4.1.9.1 To deliver limited promotional or informational communications regarding similar products and services, subject always to opt-in consent where required (GDPR; PECR/UK GDPR).

4.1.9.2 Consent may be withdrawn at any time, without prejudice to prior lawful Processing.

4.1.10 Other Purposes Based on Consent

4.1.10.1 To Process Personal Data for any additional purpose for which explicit, informed consent has been obtained, including but not limited to precise geolocation services, biometric verification, or processing of Special Categories of Data, all mutatis mutandis in line with Applicable Law.

4.1.11 Affiliate and Referral Tracking

4.1.11.1 To attribute transactions and calculate commissions for Influencers and Affiliates through referral links, influencer codes, cookies, or click-tracking identifiers.

4.1.11.2 Such Processing is limited to attribution, settlement, and anti-fraud verification, and remains subject at all times to applicable consent and opt-out mechanisms described in Sections 4 and 5.

4.1.12 Dispute Management and Refunds

4.1.12.1 To investigate, adjudicate, and process disputes, chargebacks, or refund requests.

4.1.12.2 Relevant Personal Data may be shared with Payment Service Providers, marketplaces, or contractual counterparties solely to verify claims, supply proof, and achieve equitable resolution, consistent with Section 13 (Liability and Disclaimers).

4.2 Legal Bases (EU / UK / UAE)

4.2.1 Performance of a Contract

4.2.1.1 Processing necessary for performance of a contract to which the Data Subject is party, or to take pre-contractual steps at the Data Subject's request.

4.2.2 Compliance with Legal Obligations

4.2.2.1 Processing necessary for compliance with a legal obligation to which the Company, acting as Controller, is subject under Applicable Law.

4.2.3 Legitimate Interests

4.2.3.1 Processing necessary for the legitimate interests pursued by the Company or a third party, provided however that such interests are not overridden by the Data Subject's fundamental rights or freedoms.

4.2.3.2 Legitimate interests may include fraud prevention, Service maintenance, network security, and lawful commercial communications.

4.2.4 Consent

4.2.4.1 Processing based on explicit, informed and freely given consent for activities including direct marketing, non-essential cookies, precise geolocation, or Special Category data.

4.2.4.2 Consent may be withdrawn at any time without affecting the lawfulness of prior Processing.

4.3 U.S. State Law Concepts

4.3.1 Opt-Out Rights

4.3.1.1 To honour consumer rights to opt out of targeted or cross-context behavioural advertising and certain "Sale" or "Share" of Personal Data as defined under CPRA, VCDPA, CPA, CTDPA and UCPA.

4.3.1.2 Such opt-outs are implemented through recognised Opt-Out Preference Signals or account settings, as elaborated in Exhibit 1 – Cookie Notice.

4.3.2 Verification and Exceptions

4.3.2.1 All opt-out and access rights are subject to reasonable verification and statutory exceptions, including compliance with legal obligations, establishment or defence of legal claims, or internal operations reasonably aligned with Data Subject expectations.

4.3.2.2 For the avoidance of doubt, the Company reserves the right to decline requests that would compromise platform security, reveal trade secrets, or conflict with mandatory regulatory retention obligations.

5. COOKIES, TRACKING & OPT-OUT SIGNALS

5.1 Deployment of Cookies and Similar Technologies

5.1.1 Deployment

5.1.1.1 The Services may deploy cookies, pixels, SDKs, tags, local-storage objects, device-fingerprinting technologies and analogous identifiers (collectively, "Cookies & Tracking Technologies") for the following lawful purposes:

(a) Essential operations — session management, authentication, fraud prevention and security continuity;

(b) Functional enhancements — interface personalisation, language and localisation preferences;

(c) Analytics and measurement — traffic metrics, crash diagnostics, latency monitoring and behavioural telemetry; and

(d) Advertising and cross-context behavioural profiling, provided however that the latter shall always remain subject to explicit consent or legally recognised opt-out rights, as further described herein and in Exhibit 1 — Cookie Notice.

5.1.1.2 Such instrumentation may include SDKs and telemetry modules provided by Meduza Services (for aggregated analytics) and limited cookies or session tokens deployed within PayTabs Gateway payment pages for fraud prevention and settlement logging.

5.1.2 Third-Party / PSP Cookies

5.1.2.1 Certain Cookies may be placed by authorised third parties, including Payment Service Providers and analytics/engagement SDK vendors, each operating under their own privacy notices and consent frameworks.

5.1.2.2 Where technically feasible, the Company's consent-management platform ("CMP") shall pre-block non-essential third-party Cookies in the EEA/UK until valid consent is recorded.

5.1.2.3 For PSP-hosted payment environments outside the Company's direct technical control (inter alia, PayTabs Gateway), disclosures and settings shall be surfaced to the extent feasible and otherwise governed by the PSP's mechanisms, without prejudice to the allocation of responsibilities set out in Exhibit 1 and Annex C.

5.1.3 Exhibit Reference

5.1.3.1 Categories, providers, retention periods and consent requirements are enumerated and periodically updated in Exhibit 1 — Cookie Notice, which forms an integral part of this Policy by reference.

5.2 Consent Regime

5.2.1 Non-Essential Cookies

5.2.1.1 Non-essential Cookies (including analytics, marketing and advertising identifiers) shall be deployed only after the Data Subject's prior, informed and affirmative consent, where mandated under the GDPR, ePrivacy Directive, UK PECR, or UAE PDPL.

5.2.2 Essential Cookies

5.2.2.1 Strictly necessary Cookies indispensable for the core functionality of the Services (e.g., maintaining login sessions, ensuring security, and preventing fraud) may operate without consent, pursuant to narrowly interpreted exemptions recognised under ePrivacy/PECR and UAE PDPL regimes.

5.2.3 Withdrawal of Consent

5.2.3.1 Data Subjects may withdraw consent at any time via the Cookie-preference centre, browser settings or other tools provided, without prejudice to the lawfulness of Processing based on consent before withdrawal.

5.2.4 Consent Interface (EEA/UK)

5.2.4.1 For users within the EEA or the United Kingdom, the Cookie-consent banner shall display "Accept All" and "Reject All" with equal prominence on the first-layer interface, together with a granular "Settings" option, consistent with current regulatory guidance.

5.2.5 Persistent Controls and Non-Discrimination

5.2.5.1 A persistent "Cookie Settings" link shall be available on the Services at all times to modify preferences.

5.2.5.2 Consent to non-essential Cookies shall not be a condition for accessing core Service functionalities, notwithstanding the operational necessity of Essential Cookies for basic delivery and security.

5.3 Preference and Opt-Out Signals

5.3.1 Recognition of Signals

5.3.1.1 Where required by Applicable Law, the Company shall make reasonable efforts, subject to technical feasibility, to detect, interpret and honour recognised opt-out preference signals, including, inter alia, the Global Privacy Control (GPC) and Universal Opt-Out Mechanisms (UOOM).

5.3.1.2 In jurisdictions mandating such signals (including California, Colorado and Connecticut), recognised opt-out signals shall take precedence and override conflicting on-site preferences to the extent required by law.

5.3.2 Verification and Exceptions

5.3.2.1 Honouring of such signals shall be subject to (a) verification of the Data Subject's identity where feasible, (b) technical feasibility of integration, and (c) statutory exceptions, including Processing strictly necessary for security, fraud prevention, legal compliance, or contractual performance.

5.3.3 Jurisdictional Variations

5.3.3.1 Within the European Union, explicit opt-in consent prevails.

5.3.3.2 Within U.S. states enforcing privacy statutes, recognised opt-out signals are legally binding.

5.3.3.3 Within the United Arab Emirates, explicit consent is required for any marketing or non-essential tracking; absent such consent, such tracking shall remain disabled.

5.3.3.4 For industry "Do Not Track" signals, refer to Section 2.3.5; such signals are not treated as binding unless standardised by law.

5.4 Affiliate / Referral Tracking

5.4.1 Certain cookies, pixels or referral links may be deployed exclusively for identifying referral traffic, attributing transactions, calculating commissions and performing anti-fraud checks.

5.4.2 Attribution cookies shall not be repurposed for behavioural profiling.

5.4.3 Typical retention shall not exceed twelve (12) months, unless a longer period is objectively necessary for fraud-prevention or commission-settlement cycles and such extension is expressly disclosed in Exhibit 1.

5.5 California Notice at Collection

5.5.1 For California residents, the Services provide a Notice at Collection that discloses categories of Personal Data, purposes of use, retention periods, and whether the Company "Sells" or "Shares" Personal Data (as those terms are defined under the CPRA).

5.5.2 Prominent links labelled "Do Not Sell or Share My Personal Information" and "Limit the Use of Sensitive Personal Information" shall be displayed where applicable.

5.5.3 Recognised GPC signals shall be treated as a valid opt-out request from Sale/Share to the extent required by Applicable Law.

6. SPECIAL CATEGORIES; CHILDREN

6.1 Special Categories of Personal Data

6.1.1 General Principle

6.1.1.1 The Company does not intentionally Process Special Categories of Personal Data as defined under GDPR Art. 9(1), UK GDPR Art. 10, or UAE PDPL Art. 5, save where such Processing is strictly necessary, lawful, and proportionate to a legitimate objective.

6.1.1.2 Examples may include, inter alia, Processing required for sanctions-screening, anti-money-laundering (AML) or counter-terrorist-financing (CFT) obligations, or for the fulfilment of statutory duties imposed under Applicable Law.

6.1.2 Legal Bases and Safeguards

6.1.2.1 Where Processing of Special Categories occurs, it shall be underpinned by a specific legal basis recognised by Applicable Law, including but not limited to:

(a) Explicit consent under GDPR Art. 9(2)(a);

(b) Substantial public interest under UK DPA 2018 Schedule 1; or

(c) Legal obligation or public duty under the UAE PDPL.

6.1.2.2 Such Processing shall be subject to heightened safeguards, including:

(a) pseudonymisation and encryption;

(b) restricted access on a strict "need-to-know" basis;

(c) reinforced confidentiality undertakings for authorised personnel;

(d) data-minimisation and proportionality principles; and

(e) logging and audit-trail mechanisms ensuring traceability and accountability.

6.1.3 Prohibited Processing

6.1.3.1 Notwithstanding the foregoing, Processing of Special Categories of Personal Data for marketing, advertising, or profiling purposes is categorically prohibited, save where expressly authorised by Applicable Law and supported by the Data Subject's explicit, freely given consent.

6.1.3.2 The Company shall not intentionally seek or infer any Special Category data from behaviour, content or metadata, and any incidental collection thereof shall be treated as accidental and promptly deleted upon identification.

6.2 Children's Data

6.2.1 Service Orientation

6.2.1.1 The Services are not directed towards, intended for, or designed to attract children, as defined under Applicable Law (inter alia, COPPA 15 U.S.C. §6501(1); GDPR Recital 38; UAE PDPL implementing guidance).

6.2.1.2 The Company does not design, market, or distribute products specifically targeted to minors and does not knowingly solicit information from such individuals.

6.2.2 Age Thresholds

6.2.2.1 The Company does not knowingly collect or Process Personal Data from children under:

(a) 13 years of age in the United States (per COPPA);

(b) 13–16 years of age in the European Economic Area or the United Kingdom, depending on the Member State's implementation of GDPR Art. 8; or

(c) the age threshold prescribed under UAE or other applicable local law, unless verifiable parental or guardian consent has been obtained.

6.2.3 Parental Consent Mechanisms

6.2.3.1 Where parental consent is required, the Company shall employ reasonable and proportionate measures to verify such consent, which may include:

(a) digital or written consent forms;

(b) parent/guardian identity verification;

(c) micro-charge confirmation systems; or

(d) equivalent industry-standard procedures validated under Applicable Law.

6.2.3.2 Verification data shall be stored only as long as necessary to confirm consent validity and shall thereafter be securely deleted.

6.2.4 Remedial Action

6.2.4.1 In the event that the Company becomes aware that it has inadvertently collected Personal Data from a child in contravention of this Section, it shall:

(a) delete such data without undue delay;

(b) take reasonable steps to notify the parent or legal guardian; and

(c) implement corrective measures to prevent recurrence.

6.2.4.2 These actions are undertaken in conformity with COPPA §6502(b)(1)(B) and GDPR Art. 17 (right to erasure).

6.2.5 Educational or Statutory Exceptions

6.2.5.1 For the avoidance of doubt, Processing for bona fide educational, safety, or counselling purposes may be permitted where authorised by Applicable Law, provided however that:

(a) the Processing is narrowly tailored to the permitted objective;

(b) adequate parental consent and supervision mechanisms are in place; and

(c) enhanced technical and organisational safeguards are applied.

7. DISCLOSURES; PROCESSORS; THIRD-PARTY LINKS

7.1 Engagement of Processors

7.1.1 Contractual Framework

7.1.1.1 The Company may engage duly vetted Processors — including, inter alia, cloud service providers, Payment Service Providers (PayTabs Gateway and analogous entities), analytics vendors (Meduza Services), logistics operators and communications platforms — to Process Personal Data strictly on documented instructions.

7.1.1.2 Each engagement shall be governed by a written Data Processing Agreement ("DPA") incorporating obligations no less protective than those required under GDPR Art. 28, UAE PDPL Art. 26, and their UK and U.S. counterparts.

7.1.2 Safeguards

7.1.2.1 All DPAs shall require, at minimum: (a) confidentiality undertakings; (b) implementation of appropriate technical and organisational measures; (c) restrictions on sub-processing; (d) audit

and inspection rights; (e) co-operation with supervisory authorities; and (f) secure deletion or return of Personal Data upon termination.

7.1.2.2 A high-level summary of cross-border transfer safeguards and applicable clauses (Standard Contractual Clauses, UK IDTA, DPF participation where relevant) is set forth in Annex C – International Transfers & Processor Terms.

7.2 Disclosures of Personal Data

7.2.1 Intra-Group and Affiliates

7.2.1.1 The Company may disclose Personal Data to its Affiliates and Subsidiaries for purposes consistent with this Policy, subject always to intra-group transfer agreements and, where applicable, Binding Corporate Rules (BCRs) or equivalent instruments.

7.2.2 Service Providers and Partners

7.2.2.1 Personal Data may be disclosed to payment processors, escrow services, fraud-prevention providers, IT security vendors, auditors, accountants, and professional advisors, each bound by confidentiality and data-protection obligations no less protective than those imposed on the Company itself.

7.2.2.2 Where Processing involves PayTabs Gateway (payment settlement) or Meduza Services (analytics telemetry), such third parties shall operate as independent Processors under their own privacy frameworks and certifications, and the Company shall not be liable for their independent acts or omissions.

7.2.3 Authorities and Legal Obligations

7.2.3.1 The Company may disclose Personal Data to competent governmental, supervisory, tax, law-enforcement or judicial authorities where required by Applicable Law or pursuant to valid legal requests, orders or investigations.

7.2.3.2 For the avoidance of doubt, Cookies or telemetry set on hosted payment pages remain governed by Section 5.1.2 (Third-Party / PSP Cookies) and the respective PSP's own policies.

7.2.4 Corporate Transactions

7.2.4.1 In the event of a merger, acquisition, reorganisation, or sale of assets, Personal Data may be transferred as part of the transaction, subject to assurances that protections equivalent to this Policy remain in effect.

7.2.4.2 Data Subjects shall be notified where required by law. Buyer-supplied In-Game Account Identifiers & Fulfilment Data (Section 3.1.10) may be disclosed solely as strictly necessary for such transactions and never for profiling or marketing purposes.

7.3 Third-Party Links, Storefronts and External Platforms

7.3.1 Interoperability

7.3.1.1 The Services may reference, embed, or interoperate with third-party platforms, marketplaces, influencer-operated storefronts, advertising networks and social-media integrations that function independently of the Company's infrastructure.

7.3.2 Independent Privacy Regimes

7.3.2.1 Such third-party environments are governed by their own privacy terms and data-handling practices, which may differ materially from this Policy.

7.3.2.2 Data Subjects are strongly encouraged to review the relevant third-party notices and to exercise discretion before providing any Personal Data or initiating transactions therein.

7.4 Affiliate and Referral Disclosures

7.4.1 Affiliate / Referral Tracking Data

7.4.1.1 Referral or commission-tracking data may be disclosed, subject to lawful basis and confidentiality undertakings, to influencers or their designated agents solely for the purposes of verifying commissions, settling referral fees, and maintaining performance transparency.

7.4.1.2 For the avoidance of doubt, no additional Buyer Personal Data shall be shared beyond what is strictly necessary for those purposes.

7.5 General Disclaimer Regarding Third Parties

7.5.1 Disclaimer of Liability

7.5.1.1 Notwithstanding any disclosures or engagements described in Sections 7.1–7.4, the Company expressly disclaims, to the fullest extent permitted by Applicable Law, any responsibility or liability for the acts, omissions, representations, or failures of independent processors, service providers, fulfilment partners, influencers, referral agents, external platforms or storefront operators.

7.5.1.2 Data Subjects acknowledge and agree that:

(a) such third parties are governed by their own contractual and privacy obligations, which may diverge from this Policy;

(b) the Company does not warrant or guarantee the adequacy of third-party safeguards save where mandatory law imposes joint liability; and

(c) interactions with such third parties, including purchases of in-game items or use of external services, are undertaken solely at the Data Subject's own risk and discretion.

8. INTERNATIONAL TRANSFERS

8.1 Transfer Mechanisms

8.1.1 EU Standard Contractual Clauses (SCCs)

8.1.1.1 Where Personal Data is transferred from the European Economic Area (EEA) to any jurisdiction not benefiting from an adequacy decision under GDPR Art. 45, such transfer shall be effected on the basis of the Standard Contractual Clauses adopted by the European Commission (Decision 2021/914/EU), mutatis mutandis.

8.1.1.2 Supplementary measures shall be implemented strictly to the extent required by Applicable Law.

8.1.1.3 For the avoidance of doubt, nothing herein shall be construed as a representation, warranty or admission regarding the enforceability of foreign laws, the equivalence of remedies, or the adequacy of redress mechanisms beyond statutory requirements.

8.1.2 UK International Data Transfer Agreement (IDTA) / Addendum

8.1.2.1 Where Personal Data is transferred from the United Kingdom, the Company shall rely upon either the International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs, as issued by the Information Commissioner's Office (ICO).

8.1.2.2 Such transfers shall remain subject to UK GDPR Chapter V (Arts. 44–49).

8.1.2.3 The Company expressly disclaims any obligation to adopt alternative transfer mechanisms unless mandatorily required by UK law or supervisory direction.

8.1.3 Intra-Group Agreements and Binding Corporate Rules (BCRs)

8.1.3.1 Intra-group or affiliate transfers may, where operationally feasible, be governed by Binding Corporate Rules (BCRs) or intra-group transfer agreements consistent with GDPR Art. 47 and UAE PDPL Art. 22.

8.1.3.2 The establishment or continuation of such frameworks shall remain subject to the Company's sole discretion and business judgment, without creating any perpetual or vested right of reliance.

8.1.4 Certifications and Frameworks

8.1.4.1 Transfers to the United States may, where applicable, rely upon the EU–US Data Privacy Framework (DPF), the UK Extension to the DPF, and/or the Swiss–US DPF, provided that the recipient is duly certified at the time of transfer and maintains such certification.

8.1.4.2 The Company expressly disclaims liability for any lapse, suspension, or revocation of such certifications by the recipient, the U.S. Department of Commerce, or any other competent authority.

8.1.4.3 No representation is made that continued participation under the DPF ensures equivalence with EEA/UK safeguards absent express adequacy recognition.

8.1.5 Annex Reference

8.1.5.1 A detailed summary of transfer mechanisms, jurisdiction-specific adaptations, and relevant contractual clauses is set forth in Annex C — International Transfers & Processor Terms, which is incorporated herein by reference.

8.1.5.2 Notwithstanding anything to the contrary herein, Annex C shall prevail inter se in the event of any interpretive conflict with this Section.

8.2 Supplementary Measures and Transfer Impact Assessments

8.2.1 Technical and Organisational Safeguards

8.2.1.1 All International Transfers shall be accompanied by proportionate supplementary measures, including, inter alia:

(a) encryption of data in transit and at rest to recognised industry standards;

(b) access minimisation and role-based controls;

(c) pseudonymisation or tokenisation of identifiers; and

(d) continuous monitoring of data-flow integrity and risk signals.

8.2.1.2 These measures are illustrative and non-exhaustive, and may evolve without notice in accordance with best practices and regulatory guidance.

8.2.2 Transfer Impact Assessments (TIAs)

8.2.2.1 Prior to effectuating transfers, the Company may, where required by Applicable Law, conduct Transfer Impact Assessments (TIAs) to evaluate the legal regime and practical enforceability of data-protection rights in the destination jurisdiction.

8.2.2.2 Such assessments are internal, confidential, and disclosed only to competent supervisory authorities where strictly mandated.

8.2.2.3 The Company makes no representation or warranty that any third-country legal system provides protections equivalent to those of the EEA, UK or UAE, except where formally confirmed by adequacy decisions.

8.2.3 Suspension of Transfers

8.2.3.1 Notwithstanding the foregoing, the Company reserves the unilateral right to suspend, delay, or terminate any transfer where it reasonably determines that:

(a) the recipient's legal environment prevents compliance with Applicable Law;

(b) a competent authority so directs; or

(c) continuation of the transfer would expose the Company to material legal, regulatory, or operational risk.

8.2.3.2 The Company shall not be liable for any damages, loss of profit, or business interruption arising from such suspension or termination, save where liability cannot be lawfully excluded.

8.2.4 Notification of Cross-Border Transfers

8.2.4.1 Where legally required, the Company shall notify Data Subjects that their Personal Data is being transferred outside their country of residence. Such notice shall include, at minimum:

(a) the legal basis relied upon (e.g., adequacy decision, SCCs, IDTA/Addendum, BCRs, UAE PDPL mechanisms);

(b) the safeguards implemented (encryption, pseudonymisation, access-control, minimisation); and

(c) the means by which the Data Subject may obtain a copy of, or access to, relevant safeguards.

8.2.4.2 In the absence of adequate safeguards, or where such safeguards cannot be lawfully implemented, the Company shall:

(a) clearly inform the Data Subject that their data may not enjoy an equivalent level of protection; and

(b) indicate the potential risks associated with the transfer.

8.2.4.3 Such transfers shall occur only under narrow derogations or with the Data Subject's explicit, informed consent, mutatis mutandis with GDPR Art. 49 and UAE PDPL exceptions.

8.2.4.4 For the avoidance of doubt, the Company expressly disclaims any liability for differences in foreign protections, limits on enforcement, or absence of redress mechanisms, except to the extent such liability cannot be excluded under mandatory law.

9. RETENTION & DELETION

9.1 General Principle

9.1.1 Storage Limitation

9.1.1.1 The Company shall retain Personal Data no longer than is necessary for the purposes for which such data was originally collected or otherwise lawfully Processed, in accordance with the storage-limitation principle enshrined in GDPR Art. 5(1)(e), UK GDPR Art. 5(1)(e), and UAE PDPL Art. 10.

9.1.1.2 Retention shall at all times remain proportionate to legitimate business needs, statutory duties, contractual undertakings, and the purposes of collection.

9.1.1.3 For the avoidance of doubt, longer retention periods may apply where expressly mandated by Applicable Law — including, inter alia, tax, anti-money-laundering (AML/CFT), accounting, or consumer-protection regulations — or where required for the establishment, exercise, or defence of legal claims.

9.2 Statutory Retention Periods and Litigation Holds

9.2.1 Statutory Requirements

9.2.1.1 Certain categories of Personal Data are subject to fixed statutory retention periods, including but not limited to:

(a) accounting and tax records — typically six (6) to ten (10) years under EU/UK law;

(b) AML/CFT and KYC documentation — five (5) years under UAE Federal Decree-Law No. 20 of 2018 and its Implementing Regulations;

(c) employment and HR-related records — as prescribed by relevant labour-law provisions in the jurisdiction of employment.

9.2.2 Litigation and Regulatory Holds

9.2.2.1 Where litigation, arbitration, regulatory investigation, or other formal proceedings are pending or reasonably anticipated, any Personal Data that may be relevant thereto shall be preserved under legal hold, irrespective of otherwise applicable retention periods.

9.2.2.2 Such preservation shall continue until the matter is fully and finally resolved, after which the ordinary retention and deletion rules shall again apply.

9.2.2.3 Mutatis mutandis, the same rule applies to records reasonably necessary for the exercise or defence of contractual or statutory rights.

9.3 Retention Ranges and Deletion Criteria

9.3.1 General Ranges and Criteria

9.3.1.1 Generic retention ranges, deletion criteria, and related factors — including purpose limitation, contractual necessity, statutory obligations, limitation periods, operational continuity, and technical feasibility — shall be applied as required by Applicable Law and recorded in the Company's internal registers. Upon expiry of the applicable retention period, Personal Data shall be securely deleted or anonymised in line with recognised industry practices (e.g., NIST SP 800-88), unless continued storage is legally required.

9.3.2 Secure Deletion and Anonymisation

9.3.2.1 Upon expiry of the applicable retention period, the Company shall ensure that the relevant Personal Data is securely deleted, anonymised or otherwise rendered permanently inaccessible in accordance with recognised industry standards (e.g., NIST SP 800-88 Rev. 1) and internal security controls.

9.3.2.2 Where full deletion is technically infeasible, equivalent protective measures — including logical isolation, encryption, or irreversible pseudonymisation — shall be implemented to ensure that the data is no longer used or re-identified.

9.3.3 Exceptions and Residual Retention

9.3.3.1 Notwithstanding the foregoing, continued storage may occur where:

(a) such retention is expressly required by Applicable Law or regulatory order;

(b) the data remains necessary for the fulfilment of unresolved contractual obligations; or

(c) preservation is mandated to satisfy accounting, auditing, or compliance documentation requirements.

9.3.3.2 In all such cases, retention shall be limited to the minimum duration and scope necessary for the specified purpose and shall remain subject to access restrictions and security safeguards as set forth in Section 10 (Security Measures).

10. SECURITY MEASURES

10.1 Administrative, Technical and Physical Safeguards

10.1.1 General Principle

10.1.1.1 The Company may, at its sole discretion and subject always to Applicable Law, implement and maintain such administrative, technical, and physical safeguards as it deems commercially reasonable, having regard to the nature of Processing, technological feasibility, business priorities and the costs of implementation.

10.1.1.2 Nothing herein shall be construed to derogate from or diminish any mandatory duty under GDPR Art. 32, UK GDPR Art. 32 and UAE PDPL Art. 9 to adopt appropriate technical and organisational measures.

10.1.1.3 For the avoidance of doubt, no statement in this Policy shall constitute a representation or guarantee of compliance with any specific industry standard (including PCI DSS, ISO/IEC 27001, SOC 2 or any successor framework) unless explicitly confirmed in a separate executed agreement.

10.1.2 Illustrative Safeguards

10.1.2.1 Without prejudice to the foregoing, safeguards may include, inter alia, access-management controls, multi-factor authentication, confidentiality undertakings, secure-development practices, encryption of data in transit and at rest, continuous monitoring and intrusion-detection mechanisms, and physical facility protections.

10.1.2.2 Such references are descriptive and non-binding. The Company does not warrant that any specific safeguard will be adopted or maintained for any particular duration and expressly disclaims liability for any failure or lapse therein, save where liability cannot be lawfully excluded.

10.1.3 Modification and Continuity

10.1.3.1 The Company may review, amend, suspend or replace its safeguards at any time, with or without notice, to reflect technological or regulatory changes.

10.1.3.2 No statement herein creates a contractual obligation or third-party beneficiary right regarding security measures, except where such liability is expressly imposed by Applicable Law or a separate executed agreement.

10.1.4 Reference Frameworks and Annexes

10.1.4.1 High-level information on the Company's security posture is provided in this Section 10 (Security Measures) and, where relevant to cross-border Processing, in Annex C — International Transfers & Processor Terms and Exhibit 1 — Cookie Notice (telemetry and SDKs). Any descriptions herein are illustrative and non-binding, do not constitute a warranty or commitment to any specific control, certification, or duration, and may evolve without notice, subject always to Applicable Law.10.2 Responsibilities of Users and Partners

10.2 Responsibilities of Users and Partners

10.2.1 User and Partner Security Duties

10.2.1.1 Data Subjects, users, affiliates, merchants, fulfilment partners, and any other third parties interacting with the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer and/or affiliate programmes, and related technical facilitation (including escrow arrangements and marketplace integrations) acknowledge that they are solely responsible for the security of their own devices, networks, credentials, and transmissions.

10.2.1.2 They must ensure that their systems and providers implement protections commensurate with industry practice and comply with the security, account, and usage policies imposed by relevant game publishers, platform operators, or other third parties.

10.2.2 Disclaimer of Liability

10.2.2.1 To the maximum extent permitted by Applicable Law, the Company expressly disclaims all liability for security breaches or unauthorised disclosures arising from:

(a) user negligence, misconfiguration, or failure to safeguard credentials or devices;

(b) acts or omissions of third-party providers, partners, or sub-contractors;

(c) failures of networks or cloud infrastructure not exclusively controlled by the Company;

(d) events of force majeure or other circumstances beyond reasonable control;

(e) regulatory actions or sanctions imposed by third-party platforms or publishers; and

(f) risks inherent in the use of in-game platforms or services operated by independent third parties.

10.2.2.2 This disclaimer shall not apply where the Company bears responsibility as Controller for its Processors or Sub-Processors under Applicable Law or a valid DPA.

10.2.3 Account Security Policy (Contractual Duties)

10.2.3.1 Users' contractual duties regarding credential protection, device hygiene, incident reporting, and remediation are set forth in the Company's Account Security Policy (Annex to the Terms of Service).

10.2.3.2 That policy is incorporated herein for notice purposes only and shall be interpreted and enforced pursuant to the Terms of Service as a distinct contractual instrument.

10.3 Transmission Disclaimer

10.3.1 No Absolute Security Guarantee

10.3.1.1 While the Company employs commercially reasonable security measures, it makes no absolute representation or guarantee that the transmission or storage of Personal Data will be entirely secure or error-free.

10.3.1.2 The security of Personal Data may be affected by numerous factors outside the Company's control, and the Company expressly disclaims liability for such factors.

10.3.2 Limitation of Liability

10.3.2.1 Accordingly, the Company shall not be liable for any losses, damages, or claims resulting from interception, unauthorised access, alteration, or destruction of Personal Data during transmission or storage, save only where liability cannot be excluded under mandatory law.

10.3.2.2 Nothing in this Section shall limit (a) the Company's statutory breach-notification duties under Section 12 or Applicable Law, or (b) any non-excludable rights afforded to Data Subjects thereunder.11. RIGHTS OF DATA SUBJECTS

11. RIGHTS OF DATA SUBJECTS

11.1 EU / UK / UAE Rights

11.1.1 Catalogue of Rights

11.1.1.1 Data Subjects located within the European Union, the United Kingdom, or the United Arab Emirates shall, subject always to Applicable Law, enjoy the following rights concerning the Processing of their Personal Data:

(a) Right of Access — to obtain confirmation as to whether Personal Data concerning them is being Processed and to receive a copy thereof (GDPR Art. 15; PDPL Art. 13);

(b) Right to Rectification — to request correction of inaccurate or incomplete data (GDPR Art. 16; PDPL Art. 14);

(c) Right to Erasure ("Right to Be Forgotten") — to request deletion of Personal Data in specified circumstances (GDPR Art. 17; PDPL Art. 15);

(d) Right to Restriction of Processing — to require temporary limitation of Processing (GDPR Art. 18);

(e) Right to Data Portability — to receive Personal Data in a structured, commonly used, machine-readable format and to transmit it to another controller (GDPR Art. 20; PDPL Art. 17);

(f) Right to Object — to object to Processing carried out on grounds of legitimate interest or direct marketing (GDPR Art. 21; PDPL Art. 16); and

(g) Right to Withdraw Consent — to withdraw consent at any time, without affecting the lawfulness of Processing carried out prior to such withdrawal (GDPR Art. 7(3); PDPL Art. 6).

11.1.2 Limitations and Exceptions

11.1.2.1 The rights enumerated above are not absolute and may be subject to statutory exemptions and legitimate restrictions, including, inter alia:

(a) the protection of legal privilege;

(b) safeguarding of national security or public order;

(c) respect for the rights and freedoms of other individuals;

(d) overriding public-interest considerations;

(e) compliance with supervisory or regulatory requirements; and

(f) the preservation or establishment of evidence for legal proceedings.

11.1.2.2 Where the Company declines to act upon a request, it shall — to the extent required by law — provide the requester with written reasons for refusal and inform them of available avenues of redress (e.g., supervisory-authority complaint or judicial remedy).

11.1.2.3 For the avoidance of doubt, nothing herein shall oblige the Company to disclose trade secrets, proprietary algorithms, or internal risk-assessment methodologies, except where disclosure is expressly mandated by Applicable Law.

11.2 U.S. State Privacy Rights

11.2.1 Catalogue of Rights

11.2.1.1 Data Subjects resident in jurisdictions such as California (CPRA), Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Utah (UCPA), and other U.S. states that have enacted comprehensive privacy statutes may, subject to verification, exercise the following rights:

(a) access to their Personal Data;

(b) deletion of Personal Data;

(c) correction of inaccuracies;

(d) portability of Personal Data;

(e) opt-out from the Sale or Share of Personal Data;

(f) opt-out from targeted advertising or certain forms of profiling; and

(g) the right to appeal refusals to act on a request within a reasonable statutory period.

11.2.2 Verification and Authorised Agents

11.2.2.1 All requests under this Section are subject to verification of the requester's identity and authority.

11.2.2.2 Data Subjects may submit requests through duly authorised agents, provided that:

(a) the agent furnishes verifiable proof of authorisation; and

(b) the Data Subject separately confirms the request, where required by law.

11.2.2.3 The Company reserves the right to deny requests that cannot be reasonably verified or that conflict with statutory exemptions.

11.2.2.4 Further details on verification standards, authorised agent mandates, and procedural rights shall be applied as set out in this Policy and as required by Applicable Law in the relevant jurisdiction, mutatis mutandis.

11.2.3 Exemptions

11.2.3.1 Certain categories of data and Processing activities are exempt from the rights enumerated above, including but not limited to:

(a) employment-related records or data collected in the context of human-resources administration;

(b) publicly available information as defined under CPRA §1798.140(v);

(c) data subject to sector-specific statutes such as the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLBA); and

(d) Processing undertaken for internal security, fraud-prevention, or compliance purposes expressly authorised by law.

11.2.3.2 For the avoidance of doubt, the Company's obligations under this Section extend only to those categories of Personal Data for which it acts as Controller under the relevant statute; Processing performed as a Service Provider or Contractor on behalf of third parties shall be governed exclusively by the applicable DPA or statutory exemption.

12. BREACH NOTIFICATION

12.1 Supervisory Authorities

12.1.1 Notification Obligation

12.1.1.1 In the event of a Personal Data Breach, the Company shall notify the competent supervisory authority without undue delay and, where the GDPR or UK GDPR applies, in principle within seventy-two (72) hours of becoming aware of the breach (GDPR Art. 33; UK GDPR Art. 33).

12.1.1.2 In the United Arab Emirates, such notification shall be made as soon as practicable pursuant to PDPL Art. 9, taking into account:

(a) the nature, scope, and severity of the incident;

(b) the categories and sensitivity of the Personal Data affected; and

(c) any relevant guidance or instruction issued by the UAE Data Office or other competent authority.

12.1.2 Delayed Notification

12.1.2.1 Where notification cannot be made within the prescribed timeframe (e.g., seventy-two (72) hours under the GDPR/UK GDPR), the Company shall submit an initial notice to the competent authority together with a statement of the reasons for delay, followed by a supplementary notice containing the remaining information as soon as reasonably practicable.

12.1.2.2 For the avoidance of doubt, such delay shall not of itself constitute non-compliance where objectively justified by the need to verify facts, secure systems, or mitigate ongoing risk.

12.1.3 Content of Notification

12.1.3.1 Notifications to supervisory authorities shall, to the extent known at the time of submission, include:

(a) the nature of the breach, including, where possible, the categories and approximate number of Data Subjects and records affected;

(b) the likely consequences of the breach; and

(c) the measures taken or proposed to address or mitigate the breach.

12.1.3.2 The Company may, where necessary, provide the required information in phases, subject to continuing cooperation with the supervisory authority.

12.2 Data Subjects

12.2.1 High-Risk Requirement

12.2.1.1 Where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons, the Company shall notify the affected Data Subjects without undue delay (GDPR Art. 34; PDPL Art. 9).

12.2.1.2 Such notification shall describe, in clear and plain language, the nature of the breach, the likely consequences, and the measures taken or proposed by the Company to mitigate its possible adverse effects.

12.2.2 Exceptions

12.2.2.1 Notification to Data Subjects shall not be required where any of the following conditions apply:

(a) the Company has implemented appropriate technical and organisational measures, such as encryption or tokenisation, rendering the data unintelligible to unauthorised persons;

(b) subsequent remediation has eliminated the high risk to Data Subjects' rights and freedoms; or

(c) such notification would involve disproportionate effort, in which case the Company may substitute a public communication or other equally effective disclosure mechanism, mutatis mutandis with supervisory-authority guidance.

12.2.2.2 The determination of "high risk" shall be based on objective criteria including the sensitivity of data, the scale of exposure, and the probability of harm.

12.2.3 Record-Keeping and Cooperation

12.2.3.1 The Company shall document all breaches, regardless of whether notification was required, including the facts, effects, and remedial actions taken, in accordance with GDPR Art. 33(5) and PDPL Art. 9(5).

12.2.3.2 Upon request, such records shall be made available to the competent supervisory authority for inspection.

12.2.3.3 For the avoidance of doubt, nothing in this Section shall prejudice or limit any statutory breach-reporting duties under Section 10 (Security Measures) or under contractual DPAs with Processors and Sub-Processors.

13. LIABILITY; DISCLAIMERS; LIMITATIONS

13.1 No Waiver of Mandatory Duties

13.1.1 Nothing in this Policy shall operate so as to exclude, limit, or waive liability where such exclusion, limitation, or waiver is prohibited by Applicable Law, including, inter alia:

(a) liability for death or personal injury caused by gross negligence or wilful misconduct;

(b) liability arising under non-waivable consumer-protection or data-protection statutes that provide mandatory remedies; or

(c) statutory damages or private rights of action in respect of specific security breaches, where such rights are expressly conferred by law.

13.1.2 For the avoidance of doubt, all exclusions and limitations herein shall apply to the maximum extent permitted by law, and nothing shall enlarge liability beyond what is expressly required under Applicable Law.

13.2 Disclaimer of Warranties

13.2.1 The Services are provided strictly on an "as is" and "as available" basis, without warranties of any kind, express or implied, to the fullest extent permitted by law.

13.2.2 The Company expressly disclaims all implied warranties, including, inter alia, warranties of merchantability, fitness for a particular purpose, title, non-infringement, and any warranties arising from a course of dealing, usage, or trade practice.

13.2.3 Notwithstanding anything to the contrary, the Company expressly disclaims responsibility for, and shall not be held liable in respect of, the operation, security, legality, continuity, or availability of any third-party networks, fulfilment partners, influencers, marketplaces, or external platforms over which it has no ownership or control (see also Sections 7.5 and 15.3), subject always to any non-excludable statutory obligations.

13.3 Limitation of Liability

13.3.1 Excluded Categories of Damages

To the maximum extent permitted by law, the Company shall not be liable for any indirect, incidental, consequential, exemplary, special, or punitive damages, however caused and under any theory of liability, including negligence, contract, or tort.

13.3.2 Economic Loss

Without limiting the generality of the foregoing, the Company shall not be liable for loss of profits, loss of revenue, loss of business opportunities, loss of goodwill, reputational harm, or loss or corruption of data, whether direct or indirect.

13.3.3 Specific Causes

The Company shall not be liable for damages arising out of or relating to:

(a) third-party platforms, marketplaces, or networks;

(b) unauthorised access, disclosure, or breaches not directly and proximately caused by the Company's gross negligence or wilful misconduct;

(c) compliance with lawful orders, subpoenas, investigations, or governmental requests; or

(d) force majeure events or other circumstances beyond the Company's reasonable control.

These exclusions apply except to the extent liability cannot be lawfully excluded or limited under Applicable Law, including mandatory consumer-protection statutes.

13.3.4 Aggregate Cap

To the maximum extent permitted by Applicable Law, the Company's aggregate liability arising out of or in connection with this Policy or the Services (whether in contract, tort (including negligence), misrepresentation, statutory duty, or otherwise) shall not exceed the greater of:

(a) one hundred United States dollars (USD 100); or

(b) the total amount actually paid to the Company by the Data Subject for the Services during the three (3) months immediately preceding the event giving rise to the claim.

Amounts paid to or retained by third parties (including sellers, marketplaces, PSPs, and fulfilment partners) are expressly excluded from this calculation.

13.3.5 Single Cap; No Stacking

The foregoing cap constitutes a single, aggregate limit for all claims, actions, and causes of action arising from the same or related facts or circumstances and shall not be multiplied by the number of claims or claimants. Multiple claims shall not expand the cap.

13.3.6 Carve-Outs from the Cap

The Aggregate Cap in Clause 13.3.4 shall not apply to liability that cannot be lawfully limited, including (where applicable) liability for death or personal injury caused by gross negligence or wilful misconduct, nor shall it limit non-waivable statutory remedies expressly mandated by law.

13.3.7 Essential Purpose

The Parties acknowledge and agree that the exclusions and limitations of liability in this Section 13.3 form an essential basis of the bargain between them and shall apply even if any limited remedy fails of its essential purpose, to the fullest extent permitted by law.

13.3.8 Local Consumer Safeguards

If any jurisdiction prohibits exclusion of certain damages or imposes stricter limits, the foregoing exclusions and caps shall apply only to the extent permitted in that jurisdiction and shall be deemed automatically modified mutatis mutandis to conform to the minimum permissible scope.

13.4 Indemnities

13.4.1 Indemnity by Data Subjects

Data Subjects agree to indemnify, defend, and hold harmless the Company, its Affiliates, officers, directors, employees, and agents from and against any and all claims, liabilities, losses, damages, costs, and expenses (including reasonable legal fees) arising from or related to:

(a) the Data Subject's misuse of the Services;

(b) violation of this Policy or the Terms of Service;

(c) infringement or violation of third-party rights through the Data Subject's conduct or content; or

(d) disputes between the Data Subject and third-party sellers, influencers, fulfilment partners, or game publishers.

Nothing herein shall derogate from non-waivable consumer rights or mandatory protections.

13.4.2 Defence and Settlement Control

The Company shall have the right, but not the obligation, to assume the exclusive defence and control of any matter otherwise subject to indemnification.

In such case, the Data Subject agrees to cooperate fully, and no settlement that admits fault or imposes non-monetary obligations on the Company shall be entered into without its prior written consent, which shall not be unreasonably withheld.

13.5 Game Publisher and Account Sanctions (Descriptive Wording)

13.5.1 Publisher Enforcement Disclaimer

To the maximum extent permitted by Applicable Law, the Company expressly disclaims any and all liability for, and shall not be held responsible in respect of, any enforcement measures, sanctions, or penalties imposed by game publishers, platform operators, or rights holders, including, inter alia:

(a) temporary or permanent account suspension, blocking, banning, deletion, or reset;

(b) revocation, confiscation, or deactivation of digital items, currencies, or achievements;

(c) denial of access to multiplayer or online functionality; or

(d) restriction, freezing, or alteration of gameplay progress, statistics, or rankings.

All such measures are undertaken at the sole discretion of the respective publisher or platform operator, over which the Company has no ownership, control, or influence whatsoever.

13.5.2 Buyer's Autonomous Risk (Descriptive Channel Reference)

Buyers acknowledge and agree that the acquisition, possession, or use of in-game items via the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer/affiliate programmes, and related technical facilitation (including escrow arrangements and marketplace integrations) may contravene publisher terms, end-user licence agreements (EULAs), or anti-cheat rules. Proceeding with any such activity is an autonomous, voluntary, and informed decision, undertaken solely at the Buyer's own risk and discretion. For the avoidance of doubt, the Company acts solely as an Aggregator and escrow facilitator, not as a seller, developer, or licensor of the underlying game assets.

13.5.3 Loss of Accounts or Digital Assets

The Company shall not, under any circumstances, be liable for any loss, impairment, or unavailability of user accounts, including but not limited to:

(a) loss of access to a personal, rare, or sentimental ("legacy") account;

(b) deletion or deactivation of a high-value, levelled, or "boosted" account;

(c) deterioration of in-game status, items, progress, or reputation metrics; or

(d) any consequential, emotional, or reputational loss arising therefrom.

Such losses are deemed to result from the sovereign acts of game publishers and platform operators, for which the Company bears no control, responsibility, or indemnification duty.

13.5.4 Aggregator's Limited Role

The Company's role is limited to intermediary (Aggregator) functions, including escrow, order routing, and technical fulfilment between independent parties. Accordingly, the Company shall not be deemed a seller, merchant, publisher, or licensor of digital content, nor shall it assume any obligations relating to the continued operation, accessibility, or enforceability of any in-game account, asset, or publisher-controlled ecosystem.

13.5.5 Buyer's Acknowledgment

By engaging in any transaction through the Company's websites, storefronts, applications, APIs, influencer/affiliate programmes, and related technical facilitation (including escrow and marketplace integrations), each Buyer expressly acknowledges that:

(a) the use of third-party marketplaces for in-game items may be prohibited by publisher policy;

(b) the risk of account sanction or deletion is known, foreseeable, and voluntarily assumed; and

(c) the Company cannot and does not guarantee the security, persistence, or recoverability of any game account or in-game item.

13.6 No Third-Party Beneficiaries

Nothing in this Policy shall be construed to create any right enforceable by, or confer any benefit upon, any person or entity other than the Parties hereto; no third party shall be deemed a beneficiary of this Policy.

13.7 Time Bar (Contractual Limitation Period)

Without prejudice to any shorter statutory limitation period, any claim or cause of action arising out of or related to this Policy or the Services must be brought within one (1) year after such claim or cause of action accrues, failing which it shall be permanently barred, notwithstanding any contrary statute of limitations, save only where a longer period is strictly mandated by Applicable Law.

14. GOVERNING LAW; DISPUTE RESOLUTION

14.1 Governing Law

14.1.1 Choice of Law

14.1.1.1 This Policy, and any dispute, controversy, or claim arising out of or relating hereto, shall be governed by, construed, and enforced in accordance with the laws of the United Arab Emirates, specifically those in force in the Emirate of Fujairah, without regard to conflict-of-law principles that would mandate the application of the laws of another jurisdiction.

14.1.2 Mandatory Data-Protection Statutes

14.1.2.1 Notwithstanding the foregoing, nothing herein shall operate so as to derogate from or exclude the application of mandatory data-protection statutes of the jurisdiction of the Data Subject's habitual residence (including, inter alia, EU GDPR, UK GDPR, UAE PDPL, CPRA, and other applicable U.S. state privacy laws), which shall prevail in case of conflict, but solely to the extent required by such mandatory provisions.

14.1.3 Regional Precedence Rules

14.1.3.1 In the event of conflict between UAE law and mandatory EU or UK law, the latter shall prevail solely in relation to Data Subjects protected thereby.

14.1.3.2 In the event of conflict between UAE law and mandatory U.S. state privacy laws, the latter shall prevail only to the extent non-waivable by contract and strictly limited to Data Subjects domiciled in the relevant state.

14.1.4 Severability of Choice-of-Law Clause

14.1.4.1 If any portion of this choice-of-law clause is held invalid or unenforceable, the remainder shall continue in full force and effect to the maximum extent permitted by Applicable Law, mutatis mutandis.

14.2 Jurisdiction & Dispute Resolution

14.2.1 Courts of Fujairah (Primary Forum)

14.2.1.1 Subject to carve-outs, the courts of Fujairah, UAE, shall have exclusive jurisdiction over disputes arising under or in connection with this Policy.

14.2.2 Interim and Equitable Relief

14.2.2.1 Nothing herein shall prevent either Party from seeking injunctive, equitable, or interim relief in any court of competent jurisdiction to prevent irreparable harm, preserve evidence, or maintain the status quo.

14.2.3 Optional Arbitration (By Mutual Agreement)

14.2.3.1 The Company may, at its discretion and subject to mutual agreement, propose resolution of disputes by arbitration under the rules of a recognised arbitral institution seated in the UAE (e.g., DIAC/ADGM/LCIA), with proceedings conducted in English.

14.2.3.2 Any such arbitration shall not deprive Data Subjects of non-waivable statutory remedies available under Applicable Law and shall be conducted on a confidential basis unless disclosure is required by law or order of a competent authority.

14.2.4 Non-Waiver of Mandatory Remedies

14.2.4.1 For the avoidance of doubt, nothing in this Section shall be construed to limit or waive (a) rights to lodge complaints with supervisory/data-protection authorities, or (b) any non-waivable consumer or data-protection remedies afforded by Applicable Law.

14.2.5 Severability of Forum Provisions

14.2.5.1 If any forum-selection or arbitration provision herein is found unenforceable with respect to a particular dispute or person, such provision shall be modified automatically, mutatis mutandis, to the minimum extent necessary to render it enforceable, and the remainder shall continue in effect.

15. CHANGES; ENTIRE AGREEMENT

15.1 Changes to this Policy

15.1.1 The Company reserves the right, in its sole discretion but subject always to Applicable Law, to amend, modify, supplement, or replace this Policy from time to time, in order to reflect changes in legal requirements, industry practices, or the Company's Processing activities.

15.1.2 Material amendments that significantly affect Data Subjects' rights or obligations shall be notified by appropriate means, which may include conspicuous posting on the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer and/or affiliate programmes, and related technical facilitation (including escrow arrangements and

marketplace integrations), email communication to registered addresses, or in-application notifications, as required by law.

15.1.3 Unless otherwise stated, changes shall become effective upon publication. Continued use of the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer and/or affiliate programmes, and related technical facilitation (including escrow arrangements and marketplace integrations) after the effective date shall constitute acceptance of the amended Policy, provided however that where Applicable Law requires renewed consent (e.g., for new categories of Processing), such consent shall be explicitly obtained.

15.1.4 The Company shall maintain an archive of prior versions of this Policy, available upon request, to evidence compliance and transparency.

15.2 Entire Agreement

15.2.1 This Policy constitutes the entire privacy statement and agreement between the Company and the Data Subject with respect to the subject matter herein, and supersedes any prior or contemporaneous understandings, statements, or notices relating to privacy and data protection, save where Applicable Law mandates otherwise.

15.2.2 No oral statements, representations, or assurances, whether made before or after acceptance of this Policy, shall have any binding legal effect, unless expressly incorporated herein by written amendment.

15.2.3 Any provisions which by their nature are intended to survive termination (including, without limitation, Sections on Liability, Governing Law, and Retention) shall so survive and remain binding upon the Parties mutatis mutandis.

15.3 Voluntary Choice of Buyer

15.3.1 By engaging via the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer and/or affiliate programmes, and related technical facilitation (including escrow arrangements and marketplace integrations), each Buyer expressly acknowledges, understands, and accepts that the acquisition of in-game items or virtual assets carries inherent and foreseeable risks, including, inter alia, enforcement actions or sanctions imposed by game publishers, platform operators, or other rights holders (as further referenced in Section 13.5).

15.3.2 The Buyer affirms that such acquisition constitutes the Buyer's personal, voluntary, and sovereign decision, undertaken at the Buyer's sole risk and discretion.

15.3.3 The Company shall not, under any circumstances, be held responsible, liable, or obliged to compensate, refund, or indemnify the Buyer for any negative consequences, including but not limited to suspension, banning, or loss of game accounts, items, or progress, arising directly or indirectly from such acquisition, save only where liability cannot be excluded under mandatory provisions of Applicable Law.

16. PHYSICAL MERCHANDISE & FULFILMENT PARTNERS

16.1 Scope

16.1.1 Notwithstanding the primarily digital nature of the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer and/or affiliate programmes, and related technical facilitation (including escrow arrangements and marketplace integrations), the Company may, from time to time, facilitate the sale or delivery of physical merchandise ("Merchandise") through external Fulfilment Partners.

16.2 Categories of Data

16.2.1 In connection with Merchandise transactions, the Company and its Fulfilment Partners may Process the following categories of Personal Data:

(a) recipient name;

(b) shipping address;

(c) contact number and/or email;

(d) order details and tracking identifiers;

(e) delivery-confirmation data (e.g., signatures, timestamps, courier proof-of-delivery); and

(f) evidence of delivery (including screenshots, courier photos, video recordings, or functionally equivalent proofs supplied by the Fulfilment Partner).

16.3 Role Allocation

16.3.1 The Company shall act as Controller with respect to the initial collection of Buyer details.

16.3.2 Fulfilment Partners shall act as independent Controllers or Processors, depending on contractual arrangements, and shall be subject to obligations of confidentiality, security, and data-minimisation, mutatis mutandis with Applicable Law and any governing DPA.

16.4 Disclosures

16.4.1 Disclosure of shipping and contact details to Fulfilment Partners shall be strictly limited to what is necessary for packing, shipping and delivery of the Merchandise, including carrier hand-off and proof-of-delivery workflows.

16.5 Legal Bases

16.5.1 The legal bases for such Processing shall include:

(a) performance of a contract (delivery of purchased goods);

(b) compliance with statutory obligations (e.g., customs, tax, consumer-protection laws); and

(c) legitimate interests (fraud prevention, logistics optimisation), provided however that such interests are not overridden by the Data Subject's rights and freedoms.

16.6 Retention

16.6.1 Personal Data related to Merchandise fulfilment shall be retained only for as long as necessary to satisfy statutory retention periods applicable to commercial records and consumer transactions and, thereafter, shall be securely deleted or anonymised in accordance with Applicable Law and recognised industry practices.

16.7 Liability

16.7.1 To the fullest extent permitted by Applicable Law, the Company disclaims liability for the acts or omissions of Fulfilment Partners, save where mandated by non-waivable consumer rights or mandatory statutory duties. Nothing herein shall enlarge the Company's liability beyond that imposed by statute or an express written agreement.

ANNEX A — DEFINITIONS (FULL LIST)

This Annex provides the comprehensive list of definitions used throughout the Policy. Unless otherwise specified, terms shall be construed subject always to Applicable Law and mutatis mutandis across jurisdictions.

A.1 Applicable Law. All statutes, regulations, executive guidance, and judicial/administrative practices governing the Processing of Personal Data in relevant jurisdictions (including EU GDPR, UK GDPR, UAE PDPL, CPRA and state analogues), mutatis mutandis.

A.2 Affiliate. Any entity directly or indirectly controlling, controlled by, or under common control with the Company; "control" means ownership of more than fifty percent (>50%) of the voting interests.

A.3 Subsidiary. Any entity of which the Company directly or indirectly owns more than fifty percent (>50%) of the issued share capital or equivalent voting rights.

A.4 Data Subject. Any natural person who is identified or identifiable and whose Personal Data is being Processed.

A.5 Personal Data. Any information relating to an identified or identifiable natural person; anonymised or aggregated data, duly established as such under Applicable Law, is excluded.

A.6 Processing. Any operation or set of operations performed on Personal Data, automated or otherwise (including collection, recording, organisation, storage, adaptation, retrieval, consultation, use, disclosure, restriction, erasure, destruction).

A.7 Controller. The natural or legal person which, alone or jointly with others, determines the purposes and means of Processing Personal Data.

A.8 Processor. Any natural or legal person which Processes Personal Data on behalf of the Controller, subject to a written data processing agreement with obligations no less protective than GDPR Art. 28, UAE PDPL Art. 26, and analogues.

A.9 Joint Controller. Two or more entities which jointly determine the purposes and means of Processing Personal Data, subject to GDPR Art. 26.

A.10 Supervisory Authority. Any competent authority responsible for monitoring the application of data-protection law, including the UAE Data Office, EU national DPAs, the UK ICO, and relevant U.S. Attorneys General (to the extent applicable).

A.11 Special Categories of Data. The categories enumerated in GDPR Art. 9(1) and UAE PDPL Art. 5 (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic/biometric data, health data, sex life or sexual orientation).

A.12 Sensitive Personal Information (U.S.). Personal information defined as sensitive under U.S. state privacy laws (including CPRA §1798.140), such as precise geolocation, government identifiers, biometric data, racial or ethnic origin, religious beliefs, genetic data, union membership, health information, and contents of communications.

A.13 Sale/Share (U.S.). Disclosure of Personal Data for monetary or other valuable consideration (Sale) or for cross-context behavioural advertising (Share), as defined in CPRA §1798.140 and state analogues.

A.14 International Transfer. Any transmission, disclosure, routing, or access of Personal Data to a jurisdiction outside the territory of its collection, subject to GDPR Chapter V, UK GDPR Chapter V (Arts. 44–49), and UAE PDPL Art. 22.

A.15 Data Protection Impact Assessment (DPIA). A documented assessment of the impact of envisaged Processing operations on the protection of Personal Data (GDPR Art. 35; UAE PDPL Art. 21).

A.16 Transfer Impact Assessment (TIA). An assessment of the legal framework and practices in a destination country to evaluate the adequacy of protection for Personal Data, consistent with EDPB Recommendations 01/2020.

A.17 Records of Processing Activities (ROPA). An internal register of Processing maintained by the Controller or Processor (GDPR Art. 30).

A.18 Anonymisation. The irreversible process rendering Personal Data incapable of identifying a Data Subject (PDPL Art. 1; GDPR Recital 26).

A.19 Pseudonymisation. Processing such that Personal Data can no longer be attributed to a specific Data Subject without additional information kept separately under appropriate safeguards (GDPR Art. 4(5)).

A.20 Controller-to-Processor Agreement (DPA). Binding contractual terms entered into pursuant to GDPR Art. 28 and UAE PDPL Art. 26, requiring confidentiality, appropriate technical/organisational measures, sub-processor controls, and deletion/return upon termination.

A.21 Cookies & Tracking Technologies. Cookies, pixels, SDKs, tags, local-storage objects, device-fingerprinting and telemetry modules used for essential, functional, analytics or advertising purposes (see Section 5 and Exhibit 1 — Cookie Notice).

A.22 Essential Cookies. Strictly necessary identifiers indispensable for core functionality (e.g., session continuity, authentication, fraud prevention/security), typically exempt from consent under ePrivacy/PECR and recognised under PDPL.

A.23 Non-Essential Cookies. Functional, analytics or advertising identifiers requiring prior consent (EEA/UK/PDPL) or supporting opt-out rights (U.S. state laws), as applicable.

A.24 Opt-Out Preference Signals. Recognised signals (including Global Privacy Control (GPC) and Universal Opt-Out Mechanisms (UOOM)) indicating a user's choice to opt out of certain Processing (e.g., targeted advertising, Sale/Share), honoured where required by law.

A.25 Payment Service Provider (PSP). A third-party provider (e.g., PayTabs Gateway) handling payment credentials within a PCI-DSS-validated hosted environment; the Company does not collect or store raw cardholder data (e.g., PAN, CVV/CVC).

A.26 Tokenisation (Payments). Substitution of raw payment credentials with tokens or surrogates issued by a PSP; raw PAN/CVV/track data are neither collected nor stored by the Company.

A.27 Hosted Payment Pages/Fields. PSP-controlled payment interfaces where cookies/tokens may be set for session integrity and anti-fraud; such environments operate under the PSP's notices and controls (see Exhibit 1).

A.28 Analytics SDK / Telemetry Provider. A third-party analytics/diagnostics module (e.g., Meduza Services) used for aggregated metrics, crash/latency diagnostics and product improvement, subject to consent/opt-out regimes (see Exhibit 1).

A.29 Aggregator. The Company's limited role as an intermediary facilitating escrow, order routing, technical fulfilment, risk-mitigation and integrations; the Company is not a game publisher, developer, licensor or direct seller of digital goods.

A.30 Escrow Mechanism. A settlement structure in which funds are temporarily held pending delivery confirmation or dispute resolution, mitigating fraud risk and supporting equitable settlement between independent parties.

A.31 Third-Party Platforms / Storefronts. External platforms, marketplaces, influencer-operated stores, advertising networks or social-media integrations that interoperate with the Company's channels and are governed by their own privacy regimes.

A.32 Fulfilment Partners. Third-party providers engaged to pack, ship and deliver physical merchandise; role allocation (Controller/Processor) depends on contractual arrangements and Applicable Law.

A.33 In-Game Account Identifiers & Fulfilment Data. The Company does not persistently store passwords, security answers, or full credential sets. In rare, flow-specific circumstances where an external marketplace or fulfilment channel requires time-limited operational access to credentials, such access is strictly session-bound, encrypted in transit and at rest, immediately deleted upon completion of the task, and access/deletion events are logged.

A.34 Affiliate / Referral Tracking Data. Identifiers (e.g., referral links, influencer codes, click-through records) collected for the limited purposes of attribution, commission settlement and anti-fraud verification, subject to consent/opt-out mechanisms.

A.35 Proof-of-Fulfilment. Evidence sufficient to confirm delivery/receipt (e.g., timestamps, screenshots, courier proof-of-delivery, photo/video records supplied by a Fulfilment Partner).

A.36 Personal Data Breach. A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed (GDPR Art. 4(12); PDPL Art. 1).

A.37 Data Subject Access Request (DSAR). A request by a Data Subject or authorised agent to exercise rights (access, deletion, correction, portability, objection, restriction, consent withdrawal), subject to verification and statutory exceptions.

A.38 EU/UK Representative (Art. 27). The representative designated in the EEA/UK where territorial-scope rules apply and the Company lacks an establishment (see Annex B).

A.39 Data Protection Officer (DPO). The function designated where required under GDPR/UK GDPR/PDPL to advise on and monitor compliance; contact details (if appointed) are set out in Annex B.

ANNEX B — REGIONAL CONTACTS & REPRESENTATIVES

B.1 Operative Note.

The contact details in this Annex are operative only upon publication with completed entries. Placeholders must be replaced with current, verifiable information. Where GDPR/UK GDPR Article 27 applies, EU/UK Representatives shall be formally appointed in writing prior to offering goods or facilitating transactions via the Company's websites, storefronts, mobile or desktop applications, programmatic interfaces (APIs), influencer/affiliate programmes, and related technical facilitation (including escrow arrangements and marketplace integrations) to, or monitoring the behaviour of, Data Subjects in the respective jurisdictions. Mutatis mutandis with Applicable Law.

B.2 Controller Identity (for notice purposes).

SellMMO Group FZ LLE, Fujairah Creative City Free Zone, License No. 14608/2019, P.O. Box 4422, Emirate of Fujairah, UAE.

B.3 Primary Privacy / DSAR Contact.

Email: privacy@[company].tld • Postal: as per B.2 (mark "Attention: Privacy").

Note: A DSAR webform may be provided at the Company's discretion; statutory timelines commence upon successful verification (see Section 2.3).

B.4 Contacts Table (placeholders to be completed prior to publication)

Role / Requirement	Name / Entity	Address	Email / Phone	Notes
Data Protection Officer (DPO)	[Name / Firm]	[Postal address]	[email] / [phone]	Mandatory under GDPR in specified cases; recommended under UAE PDPL Art. 10.
EU Representative (Art. 27 GDPR)	[Entity name]	[Office address in EU]	[contact email / phone]	Required where no EU establishment and Art. 3(2) applies. Written mandate required.
UK Representative (Art. 27 UK GDPR)	[Entity name]	[Office address in UK]	[contact email / phone]	Required where no UK establishment and Art. 3(2) applies. Written mandate required.
UAE Local Contact (Optional)	[Name / Dept]	[Local UAE office]	[contact]	Recommended to facilitate PDPL regulator inquiries and correspondence.

B.5 Response Timeframes (summary).

(a) EU/UK: one (1) month from verification, extendable by up to two (2) months for complexity;

(b) UAE: without undue delay, within a reasonable period per PDPL guidance;

(c) U.S. states: forty-five (45) days, extendable once by forty-five (45) days where reasonably necessary.

For the avoidance of doubt, timelines run only after identity/authority verification (see Section 2.3).

B.6 Verification & Agents. Requests may be submitted by authorised agents where permitted (e.g., CPRA; VCDPA/CPA/CTDPA), subject to proof of mandate and requester confirmation, mutatis mutandis with Section 2.3.

ANNEX C — INTERNATIONAL TRANSFERS & PROCESSOR TERMS

Preamble.
This Annex shall be interpreted mutatis mutandis with the main body of the Policy and governs all cross-border transfers of Personal Data, including intra-group transfers, transfers to third-party Processors, and onward transfers, insofar as such transfers are subject to Applicable Law (including, without limitation, the GDPR, UK GDPR, Swiss FADP, and UAE PDPL). For the avoidance of doubt, the provisions of this Annex operate cumulatively with, and not in derogation of, the Company's statutory obligations. As of 3 September 2025, the EU–U.S. Data Privacy Framework (DPF) adequacy decision was upheld by the General Court of the European Union (case T-553/23, Latombe v Commission), notwithstanding the possibility of further appeal before the Court of Justice of the EU.

C.1 Transfer Mechanisms

C.1.1 European Union (EEA origin). Cross-border transfers to third countries lacking an adequacy decision under GDPR Art. 45 shall be effected on the basis of the Standard Contractual Clauses (Commission Decision 2021/914/EU) together with supplementary measures strictly to the extent required by Applicable Law. No warranty is given as to foreign-law enforceability beyond statutory requirements.

C.1.2 United Kingdom (UK origin). Transfers shall rely upon the International Data Transfer Agreement (IDTA) or the UK Addendum to the EU SCCs (ICO templates), read with UK GDPR Chapter V (Arts. 44–49).

C.1.3 United Arab Emirates (UAE origin). Transfers shall comply with PDPL Art. 22 and related executive guidance, including reliance on adequacy determinations or, where strictly necessary and lawful, explicit consent or other narrow derogations.

C.1.4 Switzerland (FADP origin). Transfers shall follow Swiss FADP requirements and, where applicable, the Swiss Addendum to the SCCs or the Swiss–U.S. DPF (for certified recipients).

C.1.5 United States recipients / Frameworks. Where appropriate, transfers to U.S. recipients may rely upon the EU–U.S. DPF, the UK Extension to the DPF, and/or the Swiss–U.S. DPF, provided the recipient is certified at the time of transfer and maintains such certification. The Company disclaims liability for any lapse, suspension, or revocation of a recipient's certification beyond non-waivable statutory duties.

C.1.6 Onward transfers and sub-processing. Any onward transfer by a recipient or sub-processor must preserve an equivalent level of protection through appropriate contractual and technical safeguards, consistent with this Annex and Section 8 (International Transfers).

C.2 Supplementary Measures (Illustrative; Non-Exhaustive)

C.2.1 Technical safeguards. Encryption in transit and at rest using industry-recognised standards; key-management controls; pseudonymisation/tokenisation of identifiers; network segmentation and transport security.

C.2.2 Organisational safeguards. Access minimisation and least-privilege role controls; vetted personnel with confidentiality undertakings; change-management and logging/monitoring proportionate to risk.

C.2.3 Operational safeguards. Data-flow governance and transfer registries; secure channels for support and escalation; incident response aligned with Section 12 (Breach Notification). Measures are descriptive and may evolve without notice.

C.3 Transfer Impact Assessments (TIAs)

C.3.1 Scope. TIAs may include: (a) mapping of data flows (origin, transit, destination, access locations); (b) country-level risk analysis (surveillance laws, redress mechanisms, enforceability of data-subject rights); and (c) mitigations (encryption, localisation, contractual warranties and audit rights).

C.3.2 Confidentiality. TIAs and underlying methodologies are internal and confidential. They may be disclosed only to competent supervisory authorities where mandated by law.

C.3.3 No representation. The Company makes no representation that third-country laws provide a level of protection equivalent to the EEA/UK/UAE, except where confirmed by formal adequacy decisions.

C.4 Records of Processing Activities (ROPA)

C.4.1 Maintenance. ROPA shall be maintained for relevant Processing pursuant to GDPR Art. 30 and PDPL Art. 20, reflecting categories of data, purposes, retention, recipients, and safeguards.

C.4.2 Internal nature. ROPA entries are internal and confidential. Summaries may be provided to authorities upon request where legally required.

C.5 Processor Obligations (High-Level DPA Terms)

C.5.1 Core duties. Each Processor/Sub-Processor shall:

(a) maintain confidentiality;

(b) implement appropriate technical and organisational measures (proportionate to risk);

(c) Process only on documented instructions for specified purposes;

(d) engage Sub-processors only with prior written approval (general or specific) and flow-down obligations no less protective;

(e) provide audit/inspection cooperation (including reasonable certifications or summaries where appropriate);

(f) delete or return Personal Data upon termination, unless retention is mandated by law (and then isolate/minimise);

(g) assist the Company with data-subject requests, security, breach notification, and TIAs where relevant;

(h) notify the Company of a Personal Data Breach without undue delay and within twenty-four (24) to seventy-two (72) hours of discovery, providing available details and ongoing updates; and

(i) document Processing and safeguards to a level sufficient to demonstrate compliance to competent authorities.

C.5.2 Liability preservation. Nothing in this Annex enlarges the Company's liability beyond what is imposed by statute or an executed agreement; Processor liability is governed by the applicable DPA and law.

C.6 Coordination with Security & Governance Instruments

C.6.1 Alignment. Cross-border safeguards shall be implemented in coordination with the Company's Security Measures set out in Section 10 and shall be interpreted in pari materia with Section 8 (International Transfers). Any supplementary security descriptions are informational only and do not create additional obligations beyond those in this Policy or Applicable Law.

C.6.2 PSPs and hosted environments. Where transfers occur via hosted payment interfaces or third-party SDKs (e.g., PayTabs Gateway; analytics/telemetry modules), those environments operate under their own notices and controls. The Company will surface disclosures to the extent feasible and rely on contractually required safeguards (see Exhibit 1 — Cookie Notice; Section 7).

C.7 Suspension, Hierarchy & Updates

C.7.1 Suspension right. The Company may suspend, delay, or terminate a transfer (or category of transfers) where: (a) legal conditions prevent compliance; (b) a competent authority so directs; or (c) continuation would expose the Company to material legal or operational risk. The Company shall not be liable for resultant interruption, save where liability cannot be lawfully excluded.

C.7.2 Annex hierarchy. Notwithstanding anything to the contrary, this Annex C shall prevail inter se in case of interpretive conflict with Section 8, solely on matters of transfer mechanics and processor terms.

C.7.3 Dynamic references. References to SCCs/IDTA/DPF/FADP include their updates, replacements, or successors. The Company may update this Annex to reflect regulatory changes without material diminution of protections afforded to Data Subjects under Applicable Law.

EXHIBIT 1 — COOKIE NOTICE

This Exhibit sets forth the categories of cookies and similar technologies deployed on the Services, together with their purposes, providers, and typical retention periods. It forms an integral part of the Policy and shall be interpreted mutatis mutandis with Section 5 (Cookies, Tracking & Opt-Out Signals) and Annex C (International Transfers & Processor Terms).

A. Categories & Purposes

Category	Purpose	Typical Retention
Strictly Necessary	Core platform functions: authentication, secure sessions, load-balancing, CSRF protection, fraud-gate during checkout.	Session or ≤ 12 months only where strictly necessary for security/fraud-prevention.
Functional / Preferences	Remember locale, UI choices, influencer/referrer code persistence; CMP state.	6–12 months.
Analytics / Performance	Usage metrics, crash diagnostics, event funnels; product improvement.	12–24 months.
Advertising / Targeting	Campaign measurement, re-engagement, affiliate attribution.	3–12 months or until opt-out (whichever is sooner).
Fraud-Prevention / Security	Device fingerprinting, velocity checks, risk scoring, PSP anti-fraud.	Up to 24 months (proportional to risk).

B. Inventory by Provider (current as of 20 September 2025)

Provider / Technology	Cookie / Identifier (examples)	Purpose	Legal Basis (EEA/UK)	Opt-Out / Controls	Typical TTL
First-Party Platform (core)	session_id, csrf_token, routing & load-balancer tokens	Session integrity, CSRF defence, availability	Essential (ePrivacy/PECR exemption)	Browser controls (deleting may impair core functions)	Session / ≤ 12 months (security-bound)
Cloudflare (CDN)	__cf_bm, __cfruid, edge cache tokens	Bot mitigation, DDoS defence, caching	Legitimate interests; essential	Browser settings; cannot opt-out where essential	Session – 30 min
Consent Management Platform (CMP)	euconsent-v2, cmp_state	Store consent/denial choices; enforce	Legal obligation / consent orchestration	Banner “Reject all / Accept all / Settings”;	6–12 months

Provider / Technology	Cookie / Identifier (examples)	Purpose	Legal Basis (EEA/UK)	Opt-Out / Controls	Typical TTL
		banner preferences		persistent "Cookie Settings" link	
Google Analytics 4	_ga, _ga_*, _gid	Analytics & performance metrics	Consent (EEA/UK); legitimate interests elsewhere where lawful	CMP toggle; Google opt-out add-on	13–24 months
Meta / Facebook Pixel	_fbp, pixel ID	Ads measurement, retargeting	Consent (EEA/UK)	CMP toggle; Meta ad prefs; GPC honoured where applicable	~3 months
Meduza SDK (analytics/engagement)	SDK token; app instance ID	In-app analytics; engagement flows	Consent (EEA/UK)	CMP; in-app settings	~12 months
Telegram / ManyChat (bots/flows)	Referral parameters; hashed chat/user ID	Referral attribution; support automation	Consent; performance of contract for support chats	Bot/app settings; unlink account	Until chat end or 12 months
Hotjar (where deployed)	_hjSession_*, _hjIncludedInSessionSample	UX diagnostics; heatmaps	Consent (EEA/UK)	CMP toggle	Up to 12 months
Affiliate Tracker	aff_id, click_id, influencer_code	Attribution; commission settlement; anti-fraud checks	Consent (EEA/UK)	CMP toggle; clear cookies	90–365 days (capped at 12 months unless fraud-cycle requires longer)
Device Fingerprinting / Risk	Device/risk token; fingerprint ID	Fraud prevention; abuse control	Legitimate interests; vital	Not applicable	6–24 months

Provider / Technology	Cookie / Identifier (examples)	Purpose	Legal Basis (EEA/UK)	Opt-Out / Controls	Typical TTL
			interests (security)	(security-essential)	
PayTabs (Hosted PSP & 3-D Secure)	PSP session IDs; anti-fraud/3DS flow identifiers set by PSP/ACS	Checkout session management; 3-D Secure flows; fraud checks	Performance of contract; legitimate interests; consent where required	PSP page controls; CMP disclosure (prior-blocking non-essential in EEA/UK where feasible)	Session (transaction-bound)

Notes & Safeguards

1. Hosted PSP Cookies. Cookies set on hosted payment pages are governed by the PSP's own privacy/consent terms; the Company does not store PAN or CVV/CVC and relies on PCI-DSS-validated hosted fields/pages.
2. Recognised Signals. Global Privacy Control (GPC) and UOOM signals are honoured where legally binding; when verified, Advertising/Analytics are disabled or restricted accordingly (see Section 5.3).
3. Cross-Border Transfers. Third-party providers may transfer data cross-border; safeguards in Annex C apply (SCCs/IDTA/DPF, supplementary measures, TIAs).
4. Change Management. This inventory is maintained and updated upon material provider/SDK changes, with the CMP reflecting current status.

C. Controls & Withdrawal

- Consent Banner (EEA/UK). First-layer displays Accept All / Reject All with equal prominence; granular "Settings."
- Cookie Settings (persistent). Always available via a footer link to modify choices or withdraw consent at any time.
- Browser / Device Controls. Standard deletion of cookies, clearing local storage, resetting advertising IDs.
- Do Not Sell/Share (California). Dedicated link; GPC treated as a valid opt-out of Sale/Share to the extent required by CPRA.
- No Dark Patterns. Consent choices are presented clearly and are not conditioned on non-essential tracking.

D. Effective Date & Change Log

- Effective date: 20 September 2025.
- Change log (material updates): addition of explicit first-party core cookie line; clarification of PSP/3-D Secure identifiers; bounded TTLs for affiliate and risk-prevention categories; GPC/UOOM precedence reiterated; persistent settings link mandated.